Attorney Docket No. 1046.1305

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Jun OGAWA

Application No.: To be Assigned | Group Art Unit: To be Assigned

Filed: February 19, 2004 | Examiner: To be Assigned

For: NAME/ADDRESS TRANSLATION DEVICE

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-091293

Filed: March 28, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Feb. 19, 2004

By: _____

Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

op1723

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２８日

出願番号
Application Number: 特願２００３－０９１２９３

[ST. 10/C]: ［ＪＰ２００３－０９１２９３］

出願人
Applicant(s): 富士通株式会社

２００３年１１月２７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９８３０３

【書類名】　特許願
【整理番号】　0252577
【提出日】　平成15年 3月28日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明の名称】　名前／アドレス変換装置
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小川　淳
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【弁理士】
【氏名又は名称】　松倉　秀実
【連絡先】　０３－３６６９－６５７１
【手数料の表示】
【予納台帳番号】　012092
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　名前／アドレス変換装置

【特許請求の範囲】

【請求項１】

通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、

前記判定手段の判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第２判定手段と、

前記第２判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段と、

を含む名前／アドレス変換装置。

【請求項２】

第１ネットワーク及び第２ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別手段と、

前記通信元が前記第１ネットワークに属し且つ前記通信先が前記第２ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索手段と、

前記通信先のアドレスを含む回答を送出する送出手段とを含み、

前記送出手段は、前記通信元が前記第２ネットワークに属し且つ前記通信先が前記第１ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない

名前／アドレス変換装置。

【請求項３】

前記送出手段は、前記第１ネットワークに属する通信元と前記第２ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

請求項２記載の名前／アドレス変換装置。

【請求項４】

前記第１ネットワークに属する通信元に相当する第１端末に対して前記第２ネットワークに属する通信先に相当する第２端末のアドレスが回答される場合に、前記第１ネットワークと前記第２ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第１ネットワークと前記第２ネットワークとの間のアドレス変換を行う中継装置に対し、前記第１端末と前記第２端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含む

請求項２又は３記載の名前／アドレス変換装置。

【請求項５】

前記通知手段は、前記中継装置が前記第２端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第２端末の前記第２ネットワークにおけるアドレスを前記第１ネットワークのアドレスに変換するために、前記第２端末に対して仮想的に割り当てられる前記第１ネットワークのアドレスと前記第２端末の前記第２ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記送出手段は、前記第１端末が前記第２端末宛のデータに前記第２端末の前記第１ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第２端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第２端末の前記第２ネットワークにおけるアドレスに変換するために、前記第２端末の前記第１ネットワークにおけるアドレスを含む回答を送出する

請求項４記載の名前／アドレス変換装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＰネットワーク間における通信確立時のネゴシエーションに関する。

【０００２】

【従来の技術】

従来、ＩＰ（Internet Protocol）通信に関連する技術としては、以下のようなものがある。

【０００３】

（１）名前解決

ＩＰ通信を行う場合には通信元（問合せ元）端末のユーザは、一般的に通信先（問合せ先）をホスト名で指定する。このホスト名をＩＰアドレスに変換するためにＤＮＳ（Domain Name System）が用いられている。ＤＮＳは、ＴＣＰ／ＩＰネットワーク環境において、通信先（問合せ先）のホスト名（ドメイン名）から、対応するＩＰアドレスを取得できるようにするサービス、即ち「名前解決」を提供するシステムである。ＤＮＳサーバは、ホスト名とＩＰアドレスの対応関係を記述したデータベースを管理しており、クライアントからの要求に応じて、ホスト名からそのＩＰアドレスを参照できるように機能する。これにより、ユーザは、憶えにくく、分かりにくいＩＰアドレスではなく、ホスト名を指定してネットワークにアクセスすることができる。ＤＮＳの実体は分散データベースであり、図１に示すような、ドメイン・ツリーと呼ばれる構成により、膨大な数の名前とＩＰアドレスの解決を実現している。

【０００４】

図１に示されるように、ドメイン・ツリーにおいて、各ノードに位置するＤＮＳサーバは、基本的に、自身の管理するドメイン内情報とサブドメインのＤＮＳサーバ名しか知らない。そのため、ＤＮＳへの問合せ側は、ホスト名を元にこの階層を上位から順にたどっていけば、最終的にＩＰアドレス（図１では「www.forum.atmark.co.jp」のＩＰアドレス“192.X.X.X”）を知るＤＮＳサーバまでたどり着くことができる。以上のような手法により、ＩＰ通信では名前解決を実現している。

【０００５】

（２）ＩＰアドレスの種別とアドレス変換技術

ＩＰアドレスには、その割当てポリシーから「グローバルＩＰアドレス」と「

プライベートＩＰアドレス」の二種類のアドレス空間が定義されている。グローバルＩＰアドレスは、インターネットで使うことを許されたＩＰアドレスである。プライベートＩＰアドレス（RFC1918で規定）は、常時外部（Internet）への接続が必要ではない組織内部のネットワークアドレスとして自由に利用できるＩＰアドレスである。

【０００６】

この二種類のＩＰアドレスがそれぞれ定義されているプライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信では、ＮＡＴ（Network Address Translation）と呼ばれるアドレス変換手法が両空間の境界で必要になる。ＮＡＴは、社内のみで通用するプライベートＩＰアドレスと、インターネット（外部）アクセスに利用できる本来のグローバルなＩＰアドレスを相互に変換する。これによって、ローカルなＩＰアドレスしか割り当てられていないノードであっても、透過的にインターネットにアクセスすることが可能となる。

【０００７】

上述のようなＩＰアドレス変換に係る技術は、例えば、特許文献１に開示されている。

【０００８】

（３）プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信

次に、上述したプライベートＩＰアドレス空間からグローバルＩＰアドレス空間にまたがる通信の一例について説明する。図２は、プロキシ（Proxy）サーバを用いて、プライベートＩＰアドレス網からグローバルＩＰアドレス網へ通信する例を示す処理シーケンスである。

【０００９】

プロキシサーバは、図２に示されるように、社内（企業Ａ）のネットワークと外部（The Internet）の間に置かれて、データの出入りを監視するソフトウェア装置である。プロキシサーバは、データの出入りを監視するために、内部からのデータフローをアプリケーションレイヤレベルで終端し、データを精査した上で、外部への転送を行うように機能するアプリケーションレイヤにおける中継装置

として機能する。

【００１０】

プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信において、プロキシサーバを設置する目的には下記に示す３つがある。

【００１１】

（１）プロキシサーバを設置することにより、アプリケーションデータ内にある通信先（問合せ先）のホスト名をプロキシサーバが検出し、社内からの通信に適切か否かを判断する。不適切な通信であると判断された場合には、中継しないようにする。

【００１２】

即ち、プライベートＩＰアドレス網とグローバルＩＰアドレス網にまたがる通信は全てアプリケーションレイヤでの終端が必要であり、ＤＭＺ（DeMilitarized Zone）上にあるプロキシサーバ（図２でいうProxy.flab.fujitsu.com）上で特定のアプリケーション（一般的にはＨＴＴＰ）のみをアプリケーションレイヤで中継することができる。また、プロキシサーバでは、一般的に、問合せ先（通信先）の名前(ＨＴＴＰの場合はＵＲＬ（Uniform Resource Locator）中のＦＱＤＮ（Fully Qualified Domain Name：図２でいうA.outside.com））により、通信の可否を決定することができる。

【００１３】

（２）プライベートＩＰアドレス網内に存在するグローバルＩＰアドレスを送信元アドレス（SRC address）または送信先アドレス（DST address）とするパケットを流通させない。

【００１４】

即ち、プライベートＩＰアドレス網とグローバルＩＰアドレス網にまたがる通信では、グローバルＩＰアドレス網への経路制御がプライベートＩＰ網で必要になるため、プライベートＩＰ網内の経路制御が複雑になる。しかし、プロキシサーバを設けることにより、名前解決において、プライベートＩＰアドレス網からグローバルＩＰアドレス網のアドレスを取得できないようにして、グローバルＩＰアドレスの経路情報をプライベートアドレス網内に流さないようにすることが

できる。

【００１５】

（３）グローバルＩＰアドレス網上の端末からプライベートＩＰアドレス網への通信の禁止

グローバルＩＰアドレス網上の端末からプライベートＩＰアドレス網への通信を禁止することは、プライベートＩＰアドレス網とグローバルＩＰアドレス網間で通信を行うときに一般に留意すべき点として知られている。

【００１６】

従来は、ＤＮＳのドメイン・ツリー構成により、グローバルＩＰアドレス網上からプライベートＩＰアドレス網内にある端末の名前解決を実施しないようにする、または、ＤＭＺ上に存在するアドレス変換装置によりグローバルＩＰアドレス網上にある端末を問合せ元（通信元）とするパケットを破棄するなどして、グローバルＩＰアドレス網上の端末からプライベートＩＰアドレス網への通信を禁止していた。

【００１７】

その他、ＩＰアドレス変換に係る技術としては、特許文献２に開示された技術がある。

【００１８】

【特許文献１】

特開２０００－１５６７１０号公報

【特許文献２】

特開２００１－１５６８５２号公報

【００１９】

【発明が解決しようとする課題】

しかしながら、上記のような現状のアドレス空間をまたがる通信方式では下記に示すような問題があった。

【００２０】

（１）プロキシサーバの負荷

プロキシサーバは、プライベートＩＰ網内外にまたがる各々のデータフローが

流れている期間中、常に代表でアプリケーション中継をする必要があり負荷が大きくなる。

【００２１】

（２）アプリケーションの限定

プロキシサーバはアプリケーション中継を行うため、アプリケーションがプライベートＩＰ網内外にまたがる通信のサポート対象外（例えば、ＩＰ電話）となる場合には、プロキシサーバによって中継できるアプリケーションが限定されてしまう。また、特定のアプリケーションに対してプライベートＩＰ網外への通信を不許可にしたい場合には、ネットワーク管理者等がプロキシサーバを操作することによりアプリケーションが意図的に限定できてしまう。

【００２２】

本発明は上述のような問題を解決し、プロキシサーバを用いることなく（従来プロキシサーバが担っていた機能や役割を満たして）、プライベートＩＰアドレス網とグローバルＩＰアドレス網の境界上にあるＤＮＳサーバとアドレス変換装置の連携により、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信を実現することができる装置や方法を提供することを目的とする。

【００２３】

【課題を解決するための手段】

上記問題を解決するため、本発明は以下のような構成をとる。即ち、本発明の第一の態様は、名前／アドレス変換装置であって、通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、上記判定手段の判定結果に基づいて、上記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第２判定手段と、上記第２判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段とを含む。

【００２４】

本発明の第一の態様によると、名前／アドレス変換装置が、通信元から通信先

の名前に対応するアドレスの問合せを受けると、判定手段は、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元－通信先間の通信の可否を判定する。この判定結果に基づいて、第２判定手段は、上記問合せに含まれる名前に対応する通信先のアドレスを通信元に回答するか否かを判定する。通信先のアドレスを回答すると判定された場合には、回答手段は、通信先のアドレスを取得して通信元に回答する。このように第一の態様によれば、通信元と通信先との双方の条件に基づいて名前に対応するアドレスを回答するか否かを判定することができる。

【００２５】

また、本発明の第二の態様は、名前／アドレス変換装置であって、第１ネットワーク及び第２ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、上記問合せを送信した通信元、及び上記通信先がそれぞれ属するネットワークを識別する識別手段と、上記通信元が上記第１ネットワークに属し且つ上記通信先が上記第２ネットワークに属する場合には、上記通信元に対して回答すべき上記通信先のアドレスを検索する検索手段と、上記通信先のアドレスを含む回答を送出する送出手段とを含み、上記送出手段は、上記通信元が上記第２ネットワークに属し且つ上記通信先が上記第１ネットワークに属する場合には、上記通信先のアドレスを含む回答を送出しない名前／アドレス変換装置である。

【００２６】

本発明の第二の態様によると、名前／アドレス変換装置は、第１ネットワークから第２ネットワークに対して、通信先の名前に対応する通信先のアドレスの問合せが送信されると、受信手段は、上記問合せを受信する。識別手段は、受信した問合せから通信元及び通信先がそれぞれ属するネットワークを識別する。検索手段は、通信元が第１ネットワークに属し且つ通信先が第２ネットワークに属する場合には、問合せの送信元に対して回答するための通信先のアドレスを検索する。送出手段は、上記通信先のアドレスを含む回答を送出する。また、送出手段は、通信元が第２ネットワークに属し且つ通信先が第１ネットワークに属する場合には、通信先のアドレスを含む回答を送出しない。このように第二の態様によ

れば、通信元と通信先とが属するネットワーク種別を識別し、そのネットワーク種別に応じて通信先のアドレスを回答するか否かを決定することができる。即ち、第１ネットワークからは第２ネットワーク側への名前解決が行え、第２ネットワークからは第１ネットワーク側への名前解決が行えないようにすることができ、第１ネットワークの安全性を高めることができる。例えば、第１ネットワークには、プライベートＩＰアドレス網を適用し、第２ネットワークには、グローバルＩＰアドレス網を適用することができる。

【００２７】

好ましくは、第二の態様における送出手段は、上記第１ネットワークに属する通信元と上記第２ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、上記通信元へ上記通信先のアドレスを回答しないように構成することができる。

【００２８】

この場合、送出手段は、通信元と通信先間の通信で使用が許可されたアプリケーションがない場合には、通信元に対して通信先のアドレスを回答しない。これによって、第１ネットワークと第２ネットワーク間で使用が許可されていないアプリケーションの使用による通信を防止できる。

【００２９】

好ましくは、第２の態様における名前／アドレス変換装置は、上記第１ネットワークに属する通信元に相当する第１端末に対して上記第２ネットワークに属する通信先に相当する第２端末のアドレスが回答される場合に、上記第１ネットワークと上記第２ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに上記第１ネットワークと上記第２ネットワークとの間のアドレス変換を行う中継装置に対し、上記第１端末と上記第２端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含んでもよい。

【００３０】

この場合、名前／アドレス変換装置から、第２端末のアドレスが回答される場合には、通知手段は、中継装置に対して、第１－第２端末間で転送されるデータ

を通過させるための通過情報を通知する。これによって、第１ネットワークと第２ネットワーク間で転送されるデータに対し、名前／アドレス変換装置で名前解決を行った端末間のデータを通過させるように中継装置を制御することができ、中継装置において、通過が許可されていないデータを排除（遮断）することができる。

【００３１】

好ましくは、第二の態様における通知手段は、上記中継装置が上記第２端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された上記第２端末の上記第２ネットワークにおけるアドレスを上記第１ネットワークのアドレスに変換するために、上記第２端末に対して仮想的に割り当てられる上記第１ネットワークのアドレスと上記第２端末の上記第２ネットワークにおけるアドレスとを含む通過情報とを上記中継装置に通知し、上記送出手段は、上記第１端末が上記第２端末宛のデータに上記第２端末の上記第１ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ上記中継装置が上記第２端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを上記第２端末の上記第２ネットワークにおけるアドレスに変換するために、上記第２端末の上記第１ネットワークにおけるアドレスを含む回答を送出するように構成することができる。

【００３２】

この場合、通知手段は、第２端末に仮想的に割り当てられる第１ネットワークのアドレスと第２ネットワークにおけるアドレスとを中継装置に通知する。送出手段は、第１端末からの問合せに対し、第２端末の第１ネットワークにおけるアドレスを含む回答を送出する。これによって、第２ネットワークのアドレスが第１ネットワークに紛れ込むことを防止でき、また第１端末は第２端末を第１ネットワーク内の端末として認識することができる。従って、第２ネットワークの端末に仮想的に割り当てた第１ネットワーク内で使用できるアドレスを用いて、第１ネットワーク内で第２ネットワークの経路制御を行うことなく、異なる両アドレス空間の通信を実現することができ、且つ、第１ネットワークと第２ネットワークの経路の独立性を保障することができる。

【００３３】

好ましくは、第二の態様における通知手段は、上記中継装置が上記第１端末と上記第２端末との間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、上記第１端末と上記第２端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を上記中継装置に通知するように構成することができる。

【００３４】

このような場合では、中継装置は、第１端末と第２端末間の通信において、利用が許可されたアプリケーションに係るデータのみを通過させる。これによって、第１－第２端末間で利用が許可されていないアプリケーションを用いた通信を防止できる。

【００３５】

好ましくは、第２の態様における通知手段は、上記送出手段が上記第２端末のアドレスを送出する前に、上記通過情報を上記中継装置に通知するように構成することもできる。

【００３６】

この場合、第２端末のアドレスを含む回答が到着する前に、既に中継装置に当該データを通過させるための通過情報（フィルタリング情報）が登録されているように構成することができる。これによって、名前／アドレス変換装置は中継装置と連携することにより、通信元が通信先へデータを送るための動作を効率的に矛盾なく実施できるようにすることができる。

【００３７】

第２の態様において説明した送出手段及び通知手段に係る構成は、第１の態様に適用することもできる。

【００３８】

また、本発明は、コンピュータが名前／アドレス変換装置として第１及び第２の態様に示した動作を行う方法として特定することもできる。また、本発明は、コンピュータが第１及び第２の態様における名前／アドレス変換装置として機能するためのプログラム、又はこのプログラムを記録した記録媒体として特定する

こともできる。

【００３９】

本発明は、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信において、名前／アドレス変換装置が中継装置と連携するシステムに適用可能である。

【００４０】

【発明の実施の形態】

《実施形態》

以下、図面を用いて本発明の実施形態について説明する。以降、本実施形態では、名前解決を要求する通信元となる端末を問合せ元とし、名前解決要求に対し通信先となる端末を問合せ先として説明し、パケットの問合せ元を示すアドレスを送信元アドレスとし、パケットの問合せ先を示すアドレスを送信先アドレスとして説明する。なお、本実施形態の説明は例示であり、本発明の構成は以下の説明に限定されない。

【００４１】

〈概要〉

本実施形態に係るプライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信の概要を図３を用いて説明する。図３は、プライベートＩＰアドレス網からグローバルＩＰアドレス網への通信を示す図である。本実施形態では、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信において、従来プロキシサーバが担っていた機能を、プライベートＩＰアドレス網とグローバルＩＰアドレス網の境界上にあるＤＮＳサーバ（図３におけるGlobal Cを持つDNSサーバ１）とアドレス変換装置とがそれぞれ役割分担する。即ち、ＤＮＳサーバ１は、名前（通信したい端末のホスト名またはドメイン名）により接続先のフィルタリングをする役割を担い、特定の条件に合致するデータのみを通過させるように機能する。アドレス変換装置は、問合せ先のポート番号によりアプリケーションをフィルタリングする役割を担い、アドレス変換機能とフィルタリング機能とを併せ持つアドレス変換・フィルタリング装置３として機能する。なお、アドレス変換・フィルタリング装置３は、プロキシサーバのような

アプリケーションレイヤでの終端機能を有さず、アドレス変換とそれに必要なセッション管理、及びフィルタリングを行うこととする。

【００４２】

次に、本実施形態を実現するために生ずる要件についてそれぞれ説明する。

【００４３】

（１）ネットワーク構成

ネットワーク構成として、従来のネットワーク構成に追加する要件を主に説明する。

【００４４】

第一に、ＤＮＳは、その仕様上、問合せ元（通信元）端末が、問合せ先（通信先）端末がプライベートＩＰアドレス網上にあるか、グローバルＩＰアドレス網上にあるかを意識して、ＤＮＳサーバを使い分けることができない。このため、プライベートＩＰアドレス網上のＤＮＳサーバ１とグローバルＩＰアドレス網上のＤＮＳサーバ６とはドメイン・ツリー上で接続する。

【００４５】

第二に、ＤＮＳサーバ１は、プライベートＩＰアドレス網における名前解決とグローバルＩＰアドレス網における名前解決との双方を扱う必要がある。このため、ＤＮＳサーバ１は、グローバルＩＰアドレス網側のドメイン・ツリーにも属する必要がある。従って、本発明の対象となるＤＮＳサーバ１はグローバルＩＰアドレス網上(ＤＭＺ上)に配置される。

【００４６】

第三に、プライベートＩＰアドレス網はグローバルＩＰアドレス網に対する経路を有していない。このため、プライベートＩＰアドレス網からはグローバルＩＰアドレス網全体が一つのプライベートＩＰアドレス網のサブネットとして見えるように構成する。即ち、図４に示すように、企業Ａ側からみて、外部ネットワーク（The internet）が一つのサブネットに見えるように構成する。

【００４７】

以下、上記のネットワーク構成を踏まえた装置別の要件を説明する。

【００４８】

（２）ＤＮＳサーバ

次に、本発明の対象となるＤＮＳサーバ１に対して必要となる要件について説明する。

【００４９】

第一に、ＤＮＳサーバ１は、グローバルＩＰアドレス網内からの問合せであるか、またはプライベートＩＰアドレス網内からの問合せであるかを識別するための名前解決の問合せ元識別機能を有するように構成される。

【００５０】

第二に、ＤＮＳサーバ１は、名前解決の問合せ元識別情報に基づいて、プライベートＩＰアドレス網内からの名前解決の問合せのみを対象とする名前解決要求に対する回答可否を判断する機能を有するように構成される。ＤＮＳサーバ１は、プライベートＩＰアドレス網上のＤＮＳサーバ４と、グローバルＩＰアドレス網上のＤＮＳサーバ６とが接続されている。このため、例えば、図５に示すように名前解決要求の問合せ元と問合せ先（解決する名前を持つ端末の位置）に応じて名前解決要求に対する回答を変更できるように構成される。

【００５１】

名前解決要求の問合せ元と問合せ先に応じたＤＮＳサーバの回答、及び動作について図５を用いて説明する。第一に、プライベートＩＰアドレス網からプライベートＩＰアドレス網内への端末装置（ホスト）への問合せ（名前解決要求）に対しては、通常のプライベートＩＰアドレス網上のＤＮＳサーバとして動作する（図５の①に該当）。第二に、グローバルＩＰアドレス網からプライベートＩＰアドレス網内の端末装置への名前解決要求に対しては、名前解決要求を棄却する（図５の②に該当）。第三に、プライベートＩＰアドレス網からグローバルＩＰアドレス網内の端末装置への名前解決要求に対しては、接続可否を判断して回答する（図５の③に該当）。第四に、グローバルＩＰアドレス網からグローバルＩＰアドレス網内の端末装置への名前解決要求に対しては、通常のグローバルＩＰアドレス網上のＤＮＳサーバとして動作する（図５の④に該当）。

【００５２】

なお、③の動作を行うため、ＤＮＳサーバ１は、接続を許可するグローバルＩ

Ｐアドレス網上の名前毎に許可するポート番号も名前解決に必要な情報と共に管理する。この場合、ＤＮＳサーバ１は接続先のＩＰアドレスと共に対応するポート番号をアドレス変換・フィルタリング装置３に通知する。さらに、③の動作において、ＤＮＳサーバ１は、問合せ先となるグローバルＩＰアドレス網上の端末に仮想的に割り当てられたプライベートＩＰアドレスを名前解決の結果として返すように機能する。この仮想的なアドレスは、プライベートＩＰアドレス網の管理者によりＤＮＳサーバ１に予め設定される。

【００５３】

第三に、ＤＮＳサーバ１は、名前解決要求に対して回答をする場合、ＩＰアドレス（プライベートＩＰアドレス）と、そのアドレス変換の対象となるＩＰアドレス（グローバルＩＰアドレス）、及びポート番号をアドレス変換・フィルタリング装置３へ通知するためのアドレス変換・フィルタリング装置３とのネゴシエーション機能を有するように構成される。

【００５４】

（３）アドレス変換・フィルタリング装置

次に、アドレス変換・フィルタリング装置３に対して必要となる要件について説明する。アドレス変換・フィルタリング装置３は、ＤＮＳサーバ１からの通知に基づくパケットフィルタリング機能を提供する。即ち、アドレス変換・フィルタリング装置３は、プライベートＩＰアドレス側から受信するパケットに対して、転送先となるグローバルＩＰアドレス及びポート番号に基づいてフィルタリングを行い、受信したパケットを転送または廃棄する。また、アドレス変換・フィルタリング装置３は、ＮＡＴ機能を有しており、仮想的に割り当てられたプライベートＩＰアドレスとグローバルＩＰアドレスへのアドレス変換を問合せ先毎に行う。

【００５５】

〈ネットワーク構成〉

次に、本発明の実施形態を実現するためのネットワーク構成について図３を用いて説明する。

【００５６】

図３に示す例では、プライベートＩＰアドレス網として、企業Ａ内のネットワークに収容される端末（ホスト）２とＤＮＳサーバ４とを含むネットワークが示されている。また、グローバルＩＰアドレス網として、インターネットが示されており、インターネットにサーバ（ホスト）５とＤＮＳサーバ６とが接続されている。

【００５７】

プライベートＩＰアドレス網とグローバルＩＰアドレス網との間には、ネットワーク上の中間地帯（DMZ）が存在する。ネットワーク上の中間地帯には、ＤＮＳサーバ１（本発明の対象となるDNSサーバ）、アドレス変換・フィルタリング装置３、Ｌ２－ＳＷ７、ルータ８がそれぞれ配置され、プライベートＩＰアドレス網側から、アドレス変換・フィルタリング装置３、Ｌ２－ＳＷ（レイヤスイッチ）７、ルータ８の順に接続され、ＤＮＳサーバ１（本発明の対象となるDNSサーバ）は、Ｌ２－ＳＷ７に接続されている。

【００５８】

また、ネットワークを構成する各サーバや装置には、それぞれ異なるＩＰアドレス（プライベートＩＰアドレスやグローバルＩＰアドレス）が設定されている。図３に示す例では、ネットワークの中間地帯に位置するＤＮＳサーバ１には、グローバルＩＰアドレス“Ｇｌｏｂａｌ　Ｃ”とプライベートＩＰアドレス“Ｐｒｉｖａｔｅ　Ｄ”とが設定されている。また、アドレス変換・フィルタリング装置３には、グローバルＩＰアドレス“Ｇｌｏｂａｌ　Ａ”とプライベートＩＰアドレス“Ｐｒｉｖａｔｅ　Ｃ”とが設定されている。また、プライベートＩＰアドレス網内に位置するＤＮＳサーバ４には、プライベートアドレス“Ｐｒｉｖａｔｅ　Ｂ”が設定されている。また、グローバルＩＰアドレス網内に位置するＤＮＳサーバ６には、グローバルＩＰアドレス“Ｇｌｏｂａｌ　Ｅ”が設定されている。

【００５９】

また、プライベートＩＰアドレス網内の端末２とグローバルＩＰアドレス網内に存在するサーバ５には、ＩＰアドレスと特定のアプリケーションを利用する場合に使用されるポート番号とが割り当てられている。図３に示す例では、プライ

ベートＩＰアドレス網内に位置する端末２には、プライベートＩＰアドレス“Ｐｒｉｖａｔｅ　Ａ”とポート番号“Ｐｏｒｔ　ＸＸ”とが割り当てられている。また、グローバルＩＰアドレス網内に位置するサーバ５は、グローバルＩＰアドレス“Ｇｌｏｂａｌ　Ｄ”と、仮想的に割り当てられたプライベートＩＰアドレス“Ｐｒｉｖａｔｅ　Ｅ”とポート番号“Ｐｏｒｔ　ＹＹ”とが割り当てられている。また、サーバ５は、本実施形態において、問合せ先となり、名前（ホスト名またはドメイン名）として「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を有している。

【００６０】

なお、Ｌ２－ＳＷ７とルータ８は、プライベートＩＰアドレス網とグローバルＩＰアドレス網との間のトラフィックを中継する中継装置として機能する。また、Ｌ２－ＳＷ７は、ルータ８－アドレス変換・フィルタリング装置３間を転送されるパケットをＤＮＳサーバ１へ転送する、或いはＤＮＳサーバ１からのパケットをアドレス変換・フィルタリング装置３へ転送するための切替スイッチとして機能する。

【００６１】

〈ＤＮＳサーバのシステム構成〉

次に、本発明の実施形態を実現するためのＤＮＳサーバ１のシステム構成について図６を用いて説明する。図６は、ＤＮＳサーバ１のシステム構成図を示す。

【００６２】

ＤＮＳサーバ１は、通信終端部１０と、受信識別部１１と、送信パケット作成部１２と、名前解決要求問合せ元識別部１３と、名前解決要求問合せ先識別部１４と、名前解決部１５と、通信許可ポート検索部１６と、アドレス割当部１７と、アドレス返却部１８と、アドレスプール管理部１９と、名前解決回答作成部２０と、アドレス変換・フィルタリング装置への通知作成部２１とを備えている。ＤＮＳサーバ１は、パーソナルコンピュータやワークステーション等の情報処理装置を用いて構成され、その他のＤＮＳサーバ４，６と連携して問合せ先の名前（例えば、ホスト名またはドメイン名）からＩＰアドレスを取得して名前解決を図る。

【００６３】

通信終端部１０は、ネットワークからの通信を電気的に終端する。ネットワークから受信した情報はパケットとして、受信識別部１１へ渡される。また、送信パケット作成部１２からのパケットは電気的にネットワークへ送信する。

【００６４】

受信識別部１１は、パケット情報を識別する。受信識別部１１は、送信されてきたパケットに対して、二つの役割を担うように機能する。第一に、受信識別部１１は、正常パケットであるか異常パケット（例えば、フレーム形式が通常でない場合など）であるかを判断する。第二に、受信識別部１１は、名前解決要求のパケット（名前解決要求パケット）であるかアドレス返却を通知するパケット（回答パケット）であるか、それ以外のパケットであるかを判断する。

【００６５】

送信パケット作成部１２は、ネットワーク上に送信するための情報をパケット化し、通信終端部１０へ渡す。

【００６６】

名前解決要求問合せ元識別部１３は、名前解決要求の問合せ元端末がグローバルＩＰアドレス網上にあるか、またはプライベートＩＰアドレス網上にあるかを名前解決要求パケットの送信元ＩＰアドレスの種別に基づいて判断する。

【００６７】

名前解決要求問合せ先識別部１４は、名前解決をする問合せ先端末がグローバルＩＰアドレス網上にあるか、またはプライベートＩＰアドレス網上にあるかを問合せ先の名前に基づいて判断する。例えば、図６では、ドメイン名“ｆｕｊｔｓｕ．ｃｏｍ”が名前解決の問合せ先に含まれている場合にはプライベートＩＰアドレス網内の端末に対する名前の解決要求であると判断し、それ以外の場合にはグローバルＩＰアドレス網内の端末に対する名前の解決要求であると判断する。なお、ここでの判定条件（fujtsu.com）は予め指定される。

【００６８】

名前解決部１５は、名前解決要求問合せ元識別部１３と名前解決要求問合せ先識別部１４との判断結果に基づいて受信した名前解決要求が図５に示す①,②,③,④の何れに属するかを判断し、各々に対応する処理を実行する。即ち、名前解

決部１５は、名前解決要求が①に属すると判断する場合には、自身が管理する名前・アドレスデータベース１５ａ（プライベート）を検索する。また、名前解決部１５は、名前解決要求が②に属すると判断する場合には、名前解決要求を棄却する。また、名前解決部１５は、名前解決要求が③または④に属すると判断する場合には、自身が管理する名前・アドレスデータベース（グローバル）１５ｂを検索する。なお、ここでの判断条件（例えば、図５）は予め設定される。

【００６９】

各名前・アドレスデータベース１５ａ、１５ｂは、名前解決部１５と接続されている。名前・アドレスデータベース１５ａ、１５ｂは、それぞれ、問合せ先の名前とその回答であるＩＰアドレスとの対応を保持するテーブル１５ａ－１、１５ｂ－１を有する。

【００７０】

通信許可ポート検索部１６は、名前解決要求が図５に示す③に属する場合に、接続が許可されているポートを自身が管理する通信許可ポートリスト１６ａから検索する。

【００７１】

通信許可ポートリスト１６ａは、通信許可ポート検索部１６に接続されており、問合せ先の名前とその問合せ先への通信を許可するポート番号（アプリケーション）の一覧を示すテーブル１６ａ－１を有しているデータベースである。通信許可ポートリスト１６ａは、問合せ先の名前から、その名前に対して許可されているポート番号を検索して通信許可ポート検索部１６に検索結果として返す。また、検索結果が未ヒットの場合には、通信不許可とする。なお、通信許可ポートリスト１６ａの内容は、予め設定される。

【００７２】

アドレス割当部１７は、名前解決要求が図５に示す③に属する場合に、プライベートＩＰ網側に通知する名前解決要求に対する仮のアドレス（仮想のプライベートＩＰアドレス）をアドレスプール管理部１９を介してアドレスプールリスト１９ａから検索する。

【００７３】

アドレス返却部１８は、アドレス変換・フィルタリング装置３から返却されたＩＰアドレス（プライベートＩＰアドレス）をアドレスプール管理部１９を介してアドレスプールリスト１９ａに書込む。

【００７４】

アドレスプール管理部１９は、アドレスプールリスト１９ａを管理しており、アドレス割当部１７またはアドレス返却部１８と連携して、アドレスプールリスト１９ａに対するアドレス検索処理やアドレス登録処理を実行する。

【００７５】

アドレスプールリスト１９ａは、プライベートＩＰ網側に通知する名前解決要求に対する仮のアドレス（仮想のプライベートＩＰアドレス）とその割当状態との対応関係の一覧を示すテーブル１９ａ－１を有するデータベースである。割当状態は、「割当中」または「未割当」により示される。また、割当状態が「割当中」である場合には、その割当先の名前も対応させて保持する。

【００７６】

名前解決回答作成部２０は、名前解決要求の問合せ元への回答を作成する。この場合、名前解決部１５において検索に成功した場合には、解決したＩＰアドレスを内容とする回答を作成する。また、名前解決部１５において検索に失敗した場合には、名前解決の失敗を内容とする回答を作成する。

【００７７】

アドレス変換・フィルタリング装置への通知作成部２１は、名前解決要求が図５に示す③に属する場合に、アドレス変換・フィルタリング装置３への通知内容を作成する。通知内容は、第一に、通信許可ポート検索部１６で得たポート番号であり、第二に、アドレス割当部１７で得たプライベートＩＰアドレスであり、第三に、名前解決部１５で得たグローバルＩＰアドレスであり、第四に、問合せ先の名前である。

【００７８】

〈アドレス変換・フィルタリング装置のシステム構成〉

次に、本発明の実施形態を実現するためのアドレス変換・フィルタリング装置３のシステム構成について図７を用いて説明する。図７は、アドレス変換・フィ

ルタリング装置３のシステム構成図を示す。

【００７９】

アドレス変換・フィルタリング装置３は、通信終端部３１と、受信識別部３２と、送信パケット作成部３３と、フィルタ書換え部３４と、アドレス書換え・フィルタ部３６と、タイマ部３７と、設定完了通知部３８と、ＮＡＴ部３９と、返却通知作成部４０と、アドレス書換え・フィルタデータベース３５とを備えている。アドレス変換・フィルタリング装置３は、通信機能を持つパーソナルコンピュータやワークステーション等の情報処理装置を用いて構成され、ＮＡＴ（NAPT：Network Address Port Translation）によるアドレス変換機能と、受信するパケット毎のＩＰアドレス及びポート番号に基づいてそのパケットをフィルタリングする機能とを併せ持つ。

【００８０】

通信終端部３１は、ネットワークからの通信を電気的に終端する。ネットワークから受信した情報はパケットとして、受信識別部３２へ渡す。また、送信パケット作成部３３からのパケットは電気的にネットワークへ送信する。

【００８１】

受信識別部３２は、パケット情報の識別を行う。受信識別部３２では、送信されてきたパケットに対して、二つの役割を担うように機能する。第一に、受信識別部３２は、正常パケットであるか異常パケット（例えば、フレーム形式が通常でない場合など）であるかを判断する。第二に、受信識別部３２は、ＤＮＳサーバ１からの通知パケットであるか、それ以外のデータパケットであるかを判断する。

【００８２】

送信パケット作成部３３は、ネットワーク上に送信するための情報をパケット化し、通信終端部３１へ渡す。

【００８３】

フィルタ書換え部３４は、受信した通知パケットに基づいて、アドレス書換え・フィルタデータベース３５ａを書換える。書換える内容は、第一に、ＤＮＳサーバ１の通信許可ポート検索部１６で取得され、アドレス変換・フィルタリング

装置３に通知されたプライベートＩＰアドレスであり、第二に、ＤＮＳサーバ１の名前解決部１５で取得され、アドレス変換・フィルタリング装置３に通知されたグローバルＩＰアドレスであり、第三に、ＤＮＳサーバ１の通信許可ポート検索部１６で取得され、アドレス変換・フィルタリング装置３に通知されたポート番号である。

【００８４】

アドレス書換え・フィルタデータベース３５は、ＤＮＳサーバ１からの通知パケットに基づいて作成される。データベース３５は、プライベートＩＰアドレスとグローバルＩＰアドレスと、通信許可ポート番号と、最終アクセス時刻との対応を一つのエントリとした一覧を保持するテーブル３５ａを有する。また、アドレス書換え・フィルタデータベース３５は、フィルタ書換え部３４と、アドレス書換え・フィルタ部３６と、タイマ部３７とに接続されており、それぞれ連携して機能する。

【００８５】

アドレス書換え・フィルタ部３６は、データパケット毎にデータを書換える。第一に、アドレス書換え・フィルタ部３６は、プライベートＩＰアドレス網からグローバルＩＰアドレス網へのパケットに対しては、まず、パケットの送信先ＩＰアドレス（プライベートＩＰアドレス）に基づいてアドレス書換え・フィルタデータベース３５を検索し、対応するグローバルＩＰアドレスをパケットの送信先ＩＰアドレスとして書き換える。同時に、パケットの送信先ポート番号が検索結果のポート番号と一致しているか否かを確認する。一致している場合には、グローバルＩＰアドレス網へパケットを送信し、一致していない場合には、パケットを破棄する。また、アドレス書換え・フィルタ部３６は、アドレス書換え・フィルタデータベース３５における最終アクセス時刻を更新する。第二に、アドレス書換え・フィルタ部３６は、グローバルＩＰアドレス網からプライベートＩＰアドレス網へのパケットに対しては、まず、パケットの送信元ＩＰアドレス（グローバルＩＰアドレス）に基づいてアドレス書換え・フィルタデータベース３５を検索し、対応するプライベートＩＰアドレス（仮想のアドレス）をパケットの送信元ＩＰアドレスとして書換える。また、パケットの送信元ポート番号が検索

結果のポート番号と一致しているか否かを確認する。一致している場合には、プライベートＩＰアドレス網へパケットを送信し、一致していない場合には、パケットを破棄する。また、アドレス書換え・フィルタ部３６は、アドレス書換え・フィルタデータベース３５における最終アクセス時刻を更新する。

【００８６】

タイマ部３７は、アドレス書換え・フィルタデータベース３５の各エントリにおける最終アクセス時刻を定期的に確認し、一定時間アクセスされていないエントリがある場合には、該エントリを削除する。

【００８７】

設定完了通知部３８は、ＤＮＳサーバ１から受信した通知パケットに基づいてアドレス書換え・フィルタデータベース３５の書換えが終了したことをＤＮＳサーバ１に通知する情報（通知情報）を作成する。通知情報は、フィルタ書換えの終了通知と、通信許可ポート検索部１６で得たポート番号と、アドレス割当部１７で得たプライベートＩＰアドレスと、名前解決部１５で得たグローバルＩＰアドレスと、問合せ先の名前とを含む。

【００８８】

ＮＡＴ部３９は、ＮＡＴ（NAPT）処理（RFC3022に規定）を行う。即ち、ＮＡＴ部３９は、グローバルＩＰアドレスとプライベートＩＰアドレス間の変換処理を行う。

【００８９】

返却通知作成部４０は、タイマ部３７によりタイムアウトが検出されたアドレス書換え・フィルタデータベース３５の最終アクセス時刻を含むエントリを除く、他のエントリ（有効なエントリ）の情報をＤＮＳサーバ１に通知する。

【００９０】

〈パケットのデータ構造〉

次に、本実施形態において送受信されるパケットのデータ構造について図８を用いて説明する。

【００９１】

図８は、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間で送受

信されるパケットのフォーマットを示す図である。

【００９２】

図８に示されるように、パケット１００は、送信先ＩＰアドレスと送信元ＩＰアドレスと送信先ポート番号と送信元ポート番号とを示すフィールドとその他の制御情報等を示すフィールドとを含んでいる。なお、パケット１００については、本実施形態で関連する、送信先ＩＰアドレスと送信元ＩＰアドレスと送信先ポート番号と送信元ポート番号のみを取り上げて説明する。

【００９３】

プライベートＩＰアドレス網からグローバルＩＰアドレス網へ送信されるパケットは、アドレス変換・フィルタリング装置３を通過する際に、アドレス書換え・フィルタ部３６により送信先ＩＰアドレスを示すフィールドが書換えられる。また、アドレス変換・フィルタリング装置３内のＮＡＴ部３９では、通常のＮＡＴ（NAPT）処理により送信元ＩＰアドレスと送信元ポート番号とを示すフィールドが書換えられる。

【００９４】

グローバルＩＰアドレス網からプライベートＩＰアドレス網へ送信されるパケットは、アドレス変換・フィルタリング装置３を通過する際に、アドレス書換え・フィルタ部３６により送信元ＩＰアドレスを示すフィールドが書換えられる。また、アドレス変換・フィルタリング装置３内のＮＡＴ部３９では、通常のＮＡＴ（NAPT）処理により送信先ＩＰアドレスと送信先ポート番号とを示すフィールドが書換えられる。

【００９５】

〈動作フロー〉

以下、本実施形態を実現する具体的な動作について図３、図９～図１５を用いて各パターン毎に説明する。

【００９６】

〔プライベートＩＰアドレス網内からグローバルＩＰアドレス網への通信〕

（１）通信許可時

図３は、通信許可時におけるプライベートＩＰアドレス網からグローバルＩＰ

アドレス網への通信を示す処理シーケンスである。以下、図面上において、ネットワーク網間において送受信されるパケットの内容は、ＤＮＳのフロー時（名前解決要求に係る通信）には「送信元アドレス（SRC address）／送信先アドレス（DST address）／問合せまたは回答（Query or Responce）」として表す。また、データフロー時（実際のアクセス開始に係る通信）には、「送信元アドレス（SRC address）／送信先アドレス（DST address）／送信元ポート番号（SRC Port）／送信先ポート番号（DST port）」として表す。なお、図面上において、ＤＮＳのフロー時のパケットを実線で表し、データフロー時のパケットは点線で表す。

【００９７】

図３において、プライベートＩＰアドレス網（企業Ａ内のネットワーク）に収容されている端末２からグローバルＩＰアドレス網（The Internet）に収容されているサーバ５に対するパケットは、端末２とサーバ５との間に設置されているアドレス変換・フィルタリング装置３，Ｌ２－ＳＷ７，ルータ８を介してＩＰ網間を転送される。各ＤＮＳサーバ１，４，６は、端末２及びサーバ５が通信先のＩＰアドレスを知るために利用される。そして、アドレス変換・フィルタリング装置３は、ＩＰ網間を転送されるパケットのアドレス変換及びフィルタリングを司る。ここで、プライベートＩＰアドレス網（企業Ａ内のネットワーク）とグローバルＩＰアドレス網（The Internet）の間に位置するネットワーク上の中間地帯（DMZ）が、アドレス変換・フィルタリング装置３－ルータ８間（以下、グレイゾーンと呼ぶ）であると仮定して説明する。なお、端末２とサーバ５間において通信する際、Ｌ２－ＳＷ７とルータ８を経由するが、それらの動作については説明を省略する。

【００９８】

まず、プライベートＩＰアドレス網（企業Ａ内のネットワーク）に収容されている端末２からサーバ５へパケットを転送する場合には、端末２は、サーバ５のＩＰアドレスを知るために、同一ネットワーク内に存在するＤＮＳサーバ４宛に名前解決要求パケットを送信する（Ｓ１）。この場合、送信されるパケットは「Ｐｒｉｖａｔｅ　Ａ（端末２のプライベートＩＰアドレス：送信元アドレス）」

，「Ｐｒｉｖａｔｅ　Ｂ（ＤＮＳサーバ４のプライベートＩＰアドレス：送信先アドレス）」，及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ（問合せ：名前解決対象のホスト（サーバ５）の名前）」を含む。

【００９９】

次に、ＤＮＳサーバ４は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するＤＮＳサーバ１を送信先アドレスに設定した名前解決要求パケットを送信する（Ｓ２）。この時の名前解決要求パケットは「Ｐｒｉｖａｔｅ　Ｂ（ＤＮＳサーバ４のプライベートＩＰアドレス：送信元アドレス）」，「Ｐｒｉｖａｔｅ　Ｄ（ＤＮＳサーバ１のプライベートＩＰアドレス：送信先アドレス）」，及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ（問合せ：サーバ５のホスト名）」を含む。グレイゾーン上において、ＤＮＳサーバ４から送信された名前解決要求パケットは、アドレス変換・フィルタリング装置３を経由する。アドレス変換・フィルタリング装置３は、名前解決要求パケットの送信元ＩＰアドレスと送信先ＩＰアドレスとをプライベートＩＰアドレスからグローバルＩＰアドレスに変換したパケットを送信する（Ｓ３）。これによって、アドレス変換・フィルタリング装置３を通過した後の名前解決要求パケットは、「Ｇｌｏｂａｌ　Ａ（アドレス変換・フィルタリング装置３のグローバルＩＰアドレス：送信元アドレス）」，「Ｇｌｏｂａｌ　Ｃ（ＤＮＳサーバ１のグローバルＩＰアドレス：送信先アドレス）」，及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を含む。

【０１００】

続いて、グレイゾーン上に位置するＤＮＳサーバ１は、自身が持つゾーンの情報では名前解決を行うことができないので、グローバルＩＰアドレス網に収容されているＤＮＳサーバ６宛に名前解決要求パケットを送信する（Ｓ４）。この名前解決要求パケットは、「Ｇｌｏｂａｌ　Ｃ（ＤＮＳサーバ１のグローバルＩＰアドレス：送信先アドレス）」，「Ｇｌｏｂａｌ　Ｅ（ＤＮＳサーバ６のグローバルＩＰアドレス：送信先アドレス）」，及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を含む。

【０１０１】

ＤＮＳサーバ６は、ＤＮＳサーバ１から受信した名前解決要求パケットに基づ

いて名前解決を行い、その結果、サーバ５のグローバルＩＰアドレス(Ｇｌｏｂａｌ　Ｄ)を得る。そして、ＤＮＳサーバ６は、名前解決の結果を含むパケット(回答パケット)をＤＮＳサーバ１宛に送信する（Ｓ５）。即ち、名前解決要求パケットの問合せ（A.outside.com）に対応するＩＰアドレスを含む回答パケットを送信する。回答パケットは、「Ｇｌｏｂａｌ　Ｅ（送信元アドレス）」，「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」，及び「Ｇｌｏｂａｌ　Ｄ（回答：名前に対応するグローバルＩＰアドレス）」を含む。

【０１０２】

ＤＮＳサーバ１は、ＤＮＳサーバ６から回答パケットを受信する。すると、ＤＮＳサーバ１は、サーバ５の名前(ホスト名)に対して許可されているポート番号(アプリケーション識別子)を求めることで、通信を許可するか否かを判断する。ここでは、ポート番号「Ｐｏｒｔ　ＹＹ」が検索され、通信を許可すると判断したと仮定する。通信を許可する場合には、ＤＮＳサーバ１は、サーバ５に割り当てる仮想のプライベートＩＰアドレス「Ｐｒｉｖａｔｅ　Ｅ」を取得し、この「Ｐｒｉｖａｔｅ　Ｅ」と、「Ｇｏｂａｌ　Ｄ」と、「Ｐｏｒｔ　ＹＹ（通信許可ポート番号）」を含む通知パケット(登録依頼)をアドレス変換・フィルタリング装置３へ送信する（Ｓ６）。

【０１０３】

アドレス変換・フィルタリング装置３は、ＤＮＳサーバ１からの通知パケットの内容をデータベース３５に登録する。登録が完了すると、登録完了を通知するパケットをＤＮＳサーバ１に返す（Ｓ７）。

【０１０４】

ＤＮＳサーバ１は、登録完了の通知を受け取ると、ＤＮＳサーバ４への回答パケットを作成し、アドレス変換・フィルタリング装置３宛に送信する（Ｓ８）。回答パケットは、「Ｇｌｏｂａｌ　Ｃ（送信元アドレス）」，「Ｇｌｏｂａｌ　Ａ（送信先アドレス）」，及び「Ｐｒｉｖａｔｅ　Ｅ（回答：名前に対応する仮想のプライベートＩＰアドレス）」を含む。この時、ＤＮＳサーバ１は、回答として、サーバ５のグローバルＩＰアドレスを仮想のプライベートＩＰアドレスに変換する。これによって、回答パケットは、その宛先において、プライベートＩ

Ｐ網中のホストから送信されたと認識することができる。

【０１０５】

アドレス変換・フィルタリング装置３は、ＤＮＳサーバ１から受信した回答パケットの送信元アドレスと送信先アドレスをグローバルＩＰアドレスからプライベートＩＰアドレスにアドレス変換し、ＤＮＳサーバ４宛に送信する（Ｓ９）。この時、回答パケットは「Ｐｒｉｖａｔｅ　Ｄ（送信元アドレス）」,「Ｐｒｉｖａｔｅ　Ｂ（送信先アドレス）」,及び「Ｐｒｉｖａｔｅ　Ｅ」を含む。

【０１０６】

ＤＮＳサーバ４は、回答パケットを受信すると、端末２に対し、名前解決要求に対する回答パケットを送信する（Ｓ１０）。この時、回答パケットは「Ｐｒｉｖａｔｅ　Ｂ（送信元アドレス）」,「Ｐｒｉｖａｔｅ　Ａ（送信先アドレス）」,及び「Ｐｒｉｖａｔｅ　Ｅ」を含む。

【０１０７】

名前解決要求パケットを送信した端末２は、ＤＮＳサーバ４から受信した回答パケットの内容から問合せに対する回答が「Ｐｒｉｖａｔｅ　Ｅ」であることを知る。即ち、端末２は、問合せた名前（A.outside.com）に対応するＩＰアドレスが「Ｐｒｉｖａｔｅ　Ｅ」であることを知る。

【０１０８】

端末２は、サーバ５と通信を開始するために、データパケットを送信する（Ｓ１１）。この場合、データパケットのヘッダには「Ｐｒｉｖａｔｅ　Ａ（送信元アドレス）」,「Ｐｒｉｖａｔｅ　Ｅ（送信先アドレス）」,「ＸＸ（送信元ポート番号）」,及び「ＹＹ（送信先ポート番号）」が設定される。

【０１０９】

端末２から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置３を通過する。この時、アドレス変換・フィルタリング装置３は、データパケットの送信先ポート番号に基づいて通信の可否を判断し、送信先ポート番号が通信が許可されているポート番号であれば、通過可能であると判断し、このデータパケットの送信先アドレスと送信元アドレスとをプライベートＩＰアドレスからグローバルＩＰアドレスにアドレス変換して通過させる。この時

アドレス変換・フィルタリング装置３から送出されるデータパケットのヘッダは「Ｇｏｌｂａｌ　Ａ（送信元アドレス）」，「Ｇｌｏｂａｌ　Ｄ（送信先アドレス）」，「ＸＸ（送信元ポート番号）」，及び「ＹＹ（送信先ポート番号）」を含む状態となる（Ｓ１２）。

【０１１０】

サーバ５は、端末２からのデータパケットを受け取るとそのパケットの送信元である問合せ元端末２に対し、データパケットを送信する（Ｓ１３）。この場合、データパケットのヘッダは「Ｇｏｌｂａｌ　Ｄ（送信元アドレス）」，「Ｇｌｏｂａｌ　Ａ（送信先アドレス）」，「ＹＹ（送信元ポート番号）」，及び「ＸＸ（送信先ポート番号）」となる（Ｓ１３）。

【０１１１】

サーバ５から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置３を通過する。この時、データパケットの送信先アドレスと送信元アドレスは、グローバルＩＰアドレスからプライベートＩＰアドレスに変換される。これによって、アドレス変換・フィルタリング装置３から送出されるデータパケットのヘッダは「Ｐｒｉｖａｔｅ　Ｅ（送信元アドレス）」，「Ｐｒｉｖａｔｅ　Ａ（送信先アドレス）」，「ＹＹ（送信元ポート番号）」，及び「ＸＸ（送信先ポート番号）」を含む状態となる（Ｓ１４）。

【０１１２】

《Ａ－Ａ’間、及びＣ点におけるＤＮＳサーバ１の動作フロー》

次に、図３において本実施形態を実現するためのＤＮＳサーバ１の動作について図９を用いて説明する。

【０１１３】

図９は、図３におけるＤＮＳサーバ１の動作処理を示すフローチャートである。ＤＮＳサーバ１は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部１０は、ネットワーク上からのパケットを受信する（Ｓ１００）。

【０１１４】

受信識別部１１は、名前解決要求パケットであるか否か、またはアドレス変換

・フィルタリング装置３内のアドレス書換え・フィルタ部３６からのパケットであるか否かを識別する（Ｓ１０１）。

【０１１５】

この時、パケットフォーマットが異常である場合には、該パケットを破棄する（Ｓ１０２）。また、名前解決の要求・回答・アドレス返却、設定完了通知以外の正常パケットである場合には、当該パケットに応じたその他の処理を実行する（Ｓ１０３）。

【０１１６】

まず、ＤＮＳサーバ１の受信識別部１１（Ｓ１０１）において、パケットが名前解決の要求・回答であると識別された場合について説明する。Ｓ１０１において、パケットが名前解決の要求・回答であると識別された場合には、名前解決要求問合せ元識別部１３は該パケットの送信元ＩＰアドレスに基づいて問合せ元のネットワーク種別を識別する（Ｓ１０４）。続いて、パケットは名前解決要求問合せ先識別部１４に渡され、問合せ先の名前に基づいて問合せ先のネットワーク種別を識別する（Ｓ１０５）。即ち、名前解決要求問合せ元識別部１３及び名前解決要求問合せ先識別部１４は、問合せ元または問合せ先がプライベートＩＰアドレス網であるのか、グローバルＩＰアドレス網であるのかを識別する。

【０１１７】

名前解決要求問合せ元識別部１３と名前解決要求問合せ先識別部１４とによる識別結果に基づいて、名前解決部１５は、名前解決に利用するデータベースを決定する（Ｓ１０６）。即ち、図５に示すような、名前解決要求の問合せ元と問合せ先との組み合わせ条件に応じた処理を実施する。

【０１１８】

この時、問合せ元及び問合せ先が共にプライベートＩＰアドレス網又はグローバルＩＰアドレス網内に属する場合には、Ｓ１１６に処理が進み、図５の①の動作が行われる。一方、問い合わせ元がグローバルＩＰアドレス網内に属し、且つ問い合わせ先がプライベートＩＰアドレス網内に属する場合には、グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信を禁止するため、名前解決要求を棄却する(図５の②)。

【０１１９】

Ｓ１０６において、パケットの問合せ先を示すＩＰアドレスがグローバルＩＰアドレス網内のアドレスである場合、即ち、図５の③、④に該当する場合には、名前解決部１５は、名前・アドレスデータベース（グローバル）１５ｂを検索する（Ｓ１０７）。この時、ＤＮＳサーバ１は、他のＤＮＳサーバと連携し、他のＤＮＳサーバで得られる変換先のＩＰアドレスを受け取ることによって、名前解決を行うこともできる。例えば、図３に示す例では、ＤＮＳサーバ１は、ＤＮＳサーバ６との連携により、変換先のＩＰアドレス「Ｇｒｏｂａｌ　Ｄ」を得ている。

【０１２０】

Ｓ１０７において、名前解決部１５が名前・アドレスデータベース（グローバル）１５ｂを検索した結果、該当するＩＰアドレスがヒットした場合には通信許可ポート検索部１６は、名前を検索キーとして、通信許可ポートリスト１６ａから通信を許可するポート番号を検索する（Ｓ１０８）。図３に示す例では、名前に対して許可されているアプリケーションのポート番号として、「Ｐｏｒｔ　ＹＹ」が得られている。なお、Ｓ１０８の検索結果、ヒットしなかった場合（以下、「ミスヒット」と表記する）には、名前解決失敗となりＳ１１２に進む。これは、許可されていないアプリケーションの通信を排除するためである。

【０１２１】

また、Ｓ１０７において、名前解決部１５が名前・アドレスデータベース（グローバル）１５ｂを検索した結果（連携の結果を含む）、ミスヒットであった場合には、問合せ元に対する回答は名前解決失敗となり、名前解決回答作成部２０によりＤＮＳサーバ１の回答を作成する（Ｓ１１２）。

【０１２２】

Ｓ１０８の検索結果において、名前に対応するポート番号がヒットした場合には、アドレス割当部１７は、アドレスプール管理部１９を介してアドレスプールリスト１９ａからプライベート網側に割り当てるプライベートＩＰアドレスを検索する（Ｓ１０９）。図３に示す例では、Ｓ１０９において、「Ｇｒｏｂａｌ　Ｄ」に割り当てるべき仮想のプライベートＩＰアドレス「Ｐｒｉｖａｔｅ　Ｅ」

がアドレスプールリスト１９ａから得られている。Ｓ１０９の検索結果がミスヒットであった場合には、名前解決失敗となりＳ１１２に進む。

【０１２３】

Ｓ１０９の検索結果において、該当するプライベートＩＰアドレスがヒットした場合には、アドレス通知作成部２１がアドレス変換・フィルタリング装置３への通知パケット（登録依頼パケット）を作成する（Ｓ１１０）。

【０１２４】

通知パケットは、通信先のＩＰアドレス(回答)，ポート番号，送信元ＩＰアドレス，送信先ＩＰアドレス，及び名前を含む。図３に示す例では、「Ｐｒｉｖａｔｅ　Ｅ」，「Ｐｏｒｔ　ＹＹ」，「Ｇｌｏｂａｌ　Ｄ」，「Ｐｒｉｖａｔｅ　Ａ」，及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を含む通知パケットが作成されている。

【０１２５】

最終的に送信される通知パケットは、送信パケット作成部１２に渡され、通信終端部１０を経由して送信される（Ｓ１１１）。

【０１２６】

以上は、図３に示す通信許可時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図３のＡ－Ａ’間におけるＤＮＳサーバ１の動作である。ＤＮＳサーバ１は、Ａ－Ａ’間では、「Ｇｌｏｂａｌ　Ｅ」を持つＤＮＳサーバ６と連携して既存のＤＮＳ処理を行う。即ち、図９に示されるように、ＤＮＳサーバ１は、Ａ－Ａ’間において、Ｓ１００－Ｓ１０１－Ｓ１０４－Ｓ１０５－Ｓ１０６－Ｓ１０７－Ｓ１０８－Ｓ１０９－Ｓ１１０－Ｓ１１１の順に動作する。

【０１２７】

次に、ＤＮＳサーバ１の受信識別部１１（Ｓ１０１）において、パケットが設定完了通知であると識別された場合について説明する。Ｓ１０１において、受信識別部１１にてパケットが設定完了通知であると識別された場合には、名前解決回答作成部２０が、問合せ元への回答としてアドレスプールリスト１９ａから取り出したプライベートＩＰアドレスを含むＤＮＳの回答を作成する（Ｓ１１２）

。図３に示す例では、問合せ元への回答となるプライベートＩＰアドレスとして「Ｐｒｉｖａｔｅ　Ｅ」を含む回答パケットが生成される。

【０１２８】

最終的に、図３のＳ８において送信される回答パケットは、送信パケット作成部１２に渡され、通信終端部１０を経由して送信される（Ｓ１１１）。

【０１２９】

以上は、図３に示す通信許可時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図３のＣ点におけるＤＮＳサーバ１の動作である。ＤＮＳサーバ１は、Ｃ点において、アドレス変換・フィルタリング装置３からの登録完了通知パケットの受信を契機に、Ｓ１００－Ｓ１０１－Ｓ１１２－Ｓ１１１の順に動作する。

【０１３０】

《Ｂ点及びＤ点におけるアドレス変換・フィルタリング装置３の動作フロー》

次に、図３において本実施形態を実現するためのアドレス変換・フィルタリング装置３の動作について図１０を用いて説明する。

【０１３１】

図１０は、図３におけるアドレス変換・フィルタリング装置３の動作処理を示すフローチャートである。アドレス変換・フィルタリング装置３は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部３１は、ネットワーク上からのパケットを受信する（Ｓ１２０）。

【０１３２】

受信識別部３２は、正常なパケットフォーマットから構成されるデータパケット（正常なパケットフォーマットであるか否かも確認する）であるか、または、ＤＮＳサーバ１からの通知パケット（登録依頼パケット）であるかを識別する（Ｓ１２１）。

【０１３３】

Ｓ１２１において、パケットフォーマットが異常であった場合には、該パケットを破棄する（Ｓ１２２）。Ｓ１２１において、パケットがデータパケットでもなく、通知パケットでもない場合には、当該パケットに応じたその他の処理が実

行される（Ｓ１２３）。

【０１３４】

まず、アドレス変換・フィルタリング装置３内の受信識別部３２（Ｓ１２１）において、受信したパケットが通知パケットであると識別された場合について説明する。Ｓ１２１において、通知パケットであると識別された場合には、フィルタ書換え部３４に通知され、通知パケット内に含まれるプライベートＩＰアドレスとグローバルＩＰアドレスと通信許可ポート番号とをアドレス書換え・フィルタデータベース３５内に書込む（Ｓ１２４）。

【０１３５】

図３に示す例では、フィルタ書換え部３４は、通知パケットに含まれた「Ｐｒｉｖａｔｅ　Ｅ」,「Ｇｌｏｂａｌ　Ｄ」,及び「Ｐｏｒｔ　ＹＹ」がデータベースに書込まれる。

【０１３６】

続いて、設定完了通知部３８は、通知パケットに基づいてＤＮＳサーバ１への設定完了通知を作成する（Ｓ１２５）。この場合、設定完了通知は、通信先のプライベートＩＰアドレス，通信先のグローバルＩＰアドレス，通信許可ポート番号，通信先の名前，及び書換え終了通知を含む。図３に示す例では、「Ｐｒｉｖａｔｅ　Ｅ」,「Ｇｌｏｂａｌ　Ｄ」,「Ｐｏｒｔ　ＹＹ」,「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」,及び書換え終了通知を含む設定完了通知が生成される。

【０１３７】

続いて、送信パケット作成部３３は、Ｓ１２５において作成した設定完了通知をパケット化して、通信終端部３１から完了登録（図３のＳ７）としてＤＮＳサーバ１に対して送信する（Ｓ１２６）。

【０１３８】

以上は、図３に示す通信許可時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図３のＢ点におけるアドレス変換・フィルタリング装置３の動作である。即ち、アドレス変換・フィルタリング装置３は、Ｂ点において、ＤＮＳサーバ１からの通知パケットの受信（Ｓ６）を契機に、Ｓ１２０－Ｓ１２１－Ｓ１２４－Ｓ１２５－Ｓ１２６の順に動作する。

【０１３９】

次に、アドレス変換・フィルタリング装置３内の受信識別部３２（Ｓ１２１）において、受信したパケットがデータパケットであると識別された場合について説明する。Ｓ１２１において、データパケットであると識別された場合には、アドレス書換え・フィルタ部３６に通知され、アドレス書換え・フィルタ部３６はアドレス書換え・フィルタデータベース３５をデータパケットの送信先ＩＰアドレスをキーとして検索する（Ｓ１２７）。

【０１４０】

この時、アドレス書換え・フィルタ部３６は、送信元ＩＰアドレスに対応するＩＰアドレス(送信先ＩＰアドレスとしてのグローバルＩＰアドレスに対応するプライベートＩＰアドレス，または送信先ＩＰアドレスとしてのプライベートＩＰアドレスに対応するグローバルＩＰアドレス)がヒットした場合には、当該エントリに格納されているポート番号と、データパケットの送信先ポート番号とを対比し、両者が一致するか否かを判定する。そして、両者が一致する場合には、転送が許可されたデータパケットであると判定(ヒット)し、Ｓ１２８に処理を進める。これに対し、検索キーに対応するＩＰアドレスがない場合，または対応するＩＰアドレスが存在するがデータパケットの送信先ポート番号が通信許可されたポート番号に該当しない場合(ミスヒット)には、処理がＳ１３０に進む。

【０１４１】

Ｓ１２７の検索結果において、ヒットした場合には、データパケットのアドレスを書換える（Ｓ１２８）。図３に示す例では、パケットの送信先ＩＰアドレスが「Ｐｒｉｖａｔｅ　Ｅ」から「Ｇｌｏｂａｌ　Ｄ」に書換えられている。続いて、ＮＡＴ部３９において、一般的なＮＡＴ（NAPT）処理が実行される（Ｓ１２９）。送信パケット作成部３３は、Ｓ１２９においてＮＡＴ処理が施されたデータをパケット化して、通信終端部３１から送信する（Ｓ１２６）。

【０１４２】

また、Ｓ１２７の検索結果において、ミスヒットであった場合には、該パケットが破棄される（Ｓ１３０）。これによって、許可されていないＩＰアドレスへの通信や、許可されていないアプリケーションを利用した通信がフィルタリング

される。

【０１４３】

以上は、図３に示す通信許可時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図３のＤ点におけるアドレス変換・フィルタリング装置３の動作である。即ち、アドレス変換・フィルタリング装置３は、Ｄ点において、端末２からのデータパケットの受信（Ｓ１１）を契機に、Ｓ１２０－Ｓ１２１－Ｓ１２７－Ｓ１２８－Ｓ１２９－Ｓ１２６の順に動作する。

【０１４４】

本発明によれば、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間との境界上において、ＤＮＳサーバ１がアドレス変換・フィルタリング装置３と連携して両アドレス空間に必要とされる役割を分担して機能することにより、プライベートＩＰアドレス空間からグローバルＩＰアドレス空間にまたがる通信を可能にすることができる。

【０１４５】

（２）プライベートＩＰアドレスの返却

次に、プライベートＩＰアドレス網内からグローバルＩＰアドレス網内への通信（図５の③に該当）において、プライベートＩＰアドレスが返却される処理について図９、図１０、図１１を用いて説明する。

【０１４６】

図１１は、プライベートＩＰアドレスの返却処理を示す処理シーケンスである。図１１において、プライベートＩＰアドレスの返却は、データフローが一定時間流れず、アドレス変換・フィルタリング装置３のタイマ部３７によりタイムアウトが検出された場合に、アドレス変換・フィルタリング装置３からＤＮＳサーバ１に対して実行される。

【０１４７】

アドレス変換・フィルタリング装置３は、一定時間通信がない場合には、ＤＮＳサーバ１のアドレス割当部１７で得たプライベートＩＰアドレスをＤＮＳサーバ１に対して返却する（Ｓ２１）。図３に示す例では、ＤＮＳサーバ１に対して「Ｐｒｉｖａｔｅ　Ｅ」を返却される。

【０１４８】

《Ｅ点におけるアドレス変換・フィルタリング装置３の動作フロー》

次に、図１１におけるＥ点の処理について、図１０を用いて説明する。

【０１４９】

アドレス変換・フィルタリング装置３は、タイマ部３７の監視結果を契機にプライベートＩＰアドレスの返却処理を実行する。アドレス変換・フィルタリング装置３内のタイマ部３７は、定期的にアドレス書換え・フィルタデータベース３５の各エントリの更新時刻を監視する（Ｓ１３１）。Ｓ１３１の監視、またはデータフローが一定時間流れなかった場合に、タイムアウトしたエントリを検出する（Ｓ１３２）。タイムアウトしたエントリを検出した場合には、該エントリのプライベートＩＰアドレスから、返却通知作成部４０は、アドレスの返却通知を作成する（Ｓ１３３）。送信パケット作成部３３は、Ｓ１３３において作成したアドレスの返却通知をパケット化して、通信終端部３１からＤＮＳサーバ１に対してプライベートＩＰアドレスの返却通知を送信する（Ｓ１２６）。図１１に示す例では、「Ｐｒｉｖａｔｅ　Ｅ」が返却されている。

【０１５０】

以上は、図１１に示すプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図１１のＥ点におけるアドレス変換・フィルタリング装置３の動作である。即ち、アドレス変換・フィルタリング装置３は、Ｅ点において、データフローが一定時間ない場合には、Ｓ１３１－Ｓ１３２－Ｓ１３３－Ｓ１２６の順に動作する。

【０１５１】

《Ｆ点におけるＤＮＳサーバ１の動作フロー》

次に、図１１におけるＦ点の処理について、図９を用いて説明する。

【０１５２】

ＤＮＳサーバ１は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部１０は、ネットワーク上からのパケットを受信する（Ｓ１００）。

【０１５３】

受信識別部１１は、名前解決要求パケットであるか否か、またはアドレス変換・フィルタリング装置３内のアドレス書換え・フィルタ部３６からのパケットであるか否かを識別する（Ｓ１０１）。即ち、図１１のＦ点において、受信識別部１１は、受信したパケットがアドレス変換・フィルタリング装置３からのアドレス返却時のパケットであることを識別する。

【０１５４】

受信識別部１１（Ｓ１０１）において、パケットがアドレス返却であると識別されると、アドレス返却部１８は、返却するプライベートＩＰアドレスを抽出する（Ｓ１１３）。続いて、アドレス返却部１８は、アドレスプール管理部１９を介してアドレスプールリスト１９ａ内の該当するアドレスの状態を未割当に変更する（Ｓ１１４）。

【０１５５】

以上は、図１１に示すプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図１１のＦ点におけるＤＮＳサーバ１の動作である。即ち、ＤＮＳサーバ１は、Ｆ点において、データフローが一定時間ない場合には、Ｓ１００－Ｓ１０１－Ｓ１１３－Ｓ１１４の順に動作する。

【０１５６】

本発明によれば、プライベートＩＰアドレス空間とグローバルＩＰアドレス空間にまたがる通信において、一定時間通信がない場合には、実施途中である名前解決要求を終了させ、名前解決を実施しないように機能することができる。即ち、一度ＩＰアドレスを割り当てた後に一定時間通信がない場合には、アドレスを返却することにより無駄に仮想アドレスを割り当てることを防ぐことができる。

【０１５７】

（３）名前による通信拒否時

次に、名前による通信拒否時におけるプライベートＩＰアドレス網内からグローバルＩＰアドレス網内への通信（図５の③に該当）について図９、図１０、図１２を用いて説明する。

【０１５８】

図１２は、名前により通信を拒否する場合のプライベートＩＰアドレス網内か

らグローバルＩＰアドレス網内への通信を示す処理シーケンスである。ここでは、名前「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を持つサーバ５への通信を禁止する場合を想定して説明する。なお、図１２は、図３のＳ３において名前解決が拒否された場合に実行される処理であり、Ｓ３１とＳ３２は、図３のＳ１とＳ２と同じであるので説明は省略する。

【０１５９】

ＤＮＳサーバ１は、アドレス変換・フィルタリング装置３にてアドレス変換されたパケットを受信する。この時の名前解決要求パケットは「Ｇｌｏｂａｌ　Ａ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」,及び「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を含む（Ｓ３３）。

【０１６０】

ＤＮＳサーバ１は、名前解決要求パケットに含まれる名前「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を有する端末に対する通信の許可または不許可を判断する。即ち、ＤＮＳサーバ１は、通信許可ポートリスト１６ａに「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」が存在するか否かを検索する。通信許可ポートリスト１６ａに「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」が存在しなかった場合には、Ｓ３３における名前解決要求パケットに対して名前解決が拒否される。即ち、ＤＮＳサーバ１は、アドレス変換・フィルタリング装置３に対して、問合せの回答として名前解決失敗（ＥＲＲＯＲ）を含む回答パケットを送信する（Ｓ３４）。

【０１６１】

アドレス変換・フィルタリング装置３は、ＤＮＳサーバ１から受信した回答パケットの送信元アドレスと送信先アドレスをグローバルＩＰアドレスからプライベートＩＰアドレスへアドレス変換し、名前解決失敗（ＥＲＲＯＲ）を含む回答パケットをＤＮＳサーバ４宛に送信する（Ｓ３５）。

【０１６２】

ＤＮＳサーバ４は、回答パケットを受信すると、端末２に対し、名前解決要求に対する名前解決失敗（ＥＲＲＯＲ）を含む回答パケットを送信する（Ｓ３６）。

【０１６３】

《Ｇ点におけるＤＮＳサーバ１の動作フロー》

次に、図１２におけるＧ点の処理について、図９を用いて説明する。図１２のＳ１００からＳ１０７間は、図３における通信許可時のプライベートＩＰアドレス網内からグローバルＩＰアドレス網への通信と同じである。従って、図１２に示すような、名前により通信を拒否する場合の処理については、図９のＳ１０８から説明する。

【０１６４】

Ｓ１０８において、通信許可ポート検索部１６は、通信許可ポートリスト１６ａから通信を許可するポート番号を検索した結果、ヒットしなかった場合には、問合せ元に対する回答は名前解決失敗となり、名前解決回答作成部２０はＤＮＳサーバ１の回答を作成する（Ｓ１１２）。図１２に示す例では、問合せ先となる名前「Ａ．ｏｕｔｓｉｄｅ．ｃｏｍ」を検索キーとして、通信許可ポートリスト１６ａを検索し、通信を許可しているポート番号がない（ヒットしなかった）場合に、名前解決失敗となる。

【０１６５】

名前解決要求パケットに対する回答は、送信パケット作成部１２でパケット化され、通信終端部１０を経由して送信される（Ｓ１１１）。

【０１６６】

以上は、図１２に示す名前による通信拒否時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図１２のＧ点におけるＤＮＳサーバ１の動作である。即ち、名前により通信が拒否された時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、ＤＮＳサーバ１は、Ｓ１００－Ｓ１０１－Ｓ１０４－Ｓ１０５－Ｓ１０６－Ｓ１０７－Ｓ１０８－Ｓ１１２－Ｓ１１１の順に動作する。

【０１６７】

本発明によれば、プライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、問合せ先となる端末の名前（例えば、ホスト名またはドメイン名）を用いて通信を拒否することができる。

【０１６８】

（４）ポートによる通信拒否時

次に、ポートによる通信拒否時のプライベートＩＰアドレス網内からグローバルＩＰアドレス網内への通信（図５の③に該当）について図９、図１０、図１３を用いて説明する。

【０１６９】

図１３は、ポートにより通信を拒否する場合のプライベートＩＰアドレス網内からグローバルＩＰアドレス網内への通信を示す処理シーケンスである。ここでは、ポート番号として「ＺＺ」を持つサーバ５への通信を禁止する場合を想定して説明する。なお、図１３は、図３のＳ１１のパケットが拒否された場合に実行される処理であり、Ｓ４１からＳ５０間は、図３のＳ１からＳ１０と同じであるので説明は省略し、Ｓ５１から説明する。

【０１７０】

端末２は、ＤＮＳサーバ４から回答パケットを受信すると、問合せに対する回答が「Ｐｒｉｖａｔｅ　Ｅ」であることを知る。即ち、端末２は、問合せた名前（A.outside.com）に対応するＩＰアドレスが「Ｐｒｉｖａｔｅ　Ｅ」であることを知る。

【０１７１】

端末２は、サーバ５と通信を開始するために、データパケットを送信する（Ｓ５１）。この場合、データパケットのヘッダには「Ｐｒｉｖａｔｅ　Ａ（送信元ＩＰアドレス）」,「Ｐｒｉｖａｔｅ　Ｅ（送信先ＩＰアドレス）」,「ＸＸ（送信元ポート番号）」,及び「ＺＺ（送信先ポート番号）」が設定される。

【０１７２】

端末２から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置３を通過する。この時、アドレス変換・フィルタリング装置３は、データパケットの送信先ポート番号に基づいてフィルタリングを実施し、通信不可であると判断したデータパケットを破棄する。図１３に示す例では、データパケットの送信先ポート番号「ＺＺ」に対してフィルタリングを実施する。本実施形態では、ポート番号「ＺＺ」に対して通信を禁止しているため、該パケットは破棄されている。

【０１７３】

《Ｈ点におけるアドレス変換・フィルタリング装置３の動作フロー》

次に、図１３におけるＨ点の処理について、図１０を用いて説明する。図１０のＳ１２０とＳ１２１は、図３における通信許可時のプライベートＩＰアドレス網内からグローバルＩＰアドレス網内への通信と同じであるため、説明は省略しＳ１２７から説明する。

【０１７４】

Ｓ１２７において、アドレス書換え・フィルタ部３６は、アドレス書換え・フィルタデータベース３５を検索する。即ち、データパケットの送信先ＩＰアドレスをキーとしてデータベース３５を検索し、ヒットした通信許可ポート番号とデータパケットの送信先ポート番号が一致しているか否かを判断する。図１３に示す例では、データベース３５に登録されている通信許可ポート番号とデータパケットの送信先ポート番号「ＺＺ」が一致していないと判断されたため、ミスヒットとなりパケットが破棄されている（Ｓ１３０）。

【０１７５】

以上は、図１３に示すポートによる通信拒否時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、図１３のＨ点におけるアドレス変換・フィルタリング装置３の動作である。即ち、ポートにより通信が拒否された場合のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、アドレス変換・フィルタリング装置３は、Ｓ１２０－Ｓ１２１－Ｓ１２７－Ｓ１３０の順に動作する。

【０１７６】

本発明によれば、プライベートＩＰアドレス網からグローバルＩＰアドレス網への通信において、パケットがアドレス変換・フィルタリング装置３を通過する際、データパケットのポート番号に基づいて通信の可否を判断することができ、該パケットを通過させるか否かを決定することができる。

【０１７７】

〔グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信〕

次に、グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信（

図５の②に該当）について図１４を用いて説明する。

【０１７８】

図１４は、グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信を示す処理シーケンスである。図１４に示す例では、端末２に名前“Ｂ．ｉｎｓｉｄｅ．ｆｕｊｉｔｓｕ．ｃｏｍ”が設定されている。

【０１７９】

まず、グローバルＩＰアドレス網（The Internet内のネットワーク）に収容されているサーバ５から端末２へパケットを転送する場合には、サーバ５は、端末２のＩＰアドレスを知るために、同一ネットワーク内に存在するＤＮＳサーバ６宛に名前解決要求パケットを送信する（Ｓ６１）。この場合、送信されるパケットは「Ｇｌｏｂａｌ　Ｄ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」,及び「Ｂ．ｉｎｓｉｄｅ．ｆｕｊｉｔｓｕ．ｃｏｍ（問合せ：名前解決対象の端末２の名前）」となる。

【０１８０】

次に、ＤＮＳサーバ６は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するＤＮＳサーバ１を送信先アドレスに設定した名前解決要求パケットを送信する（Ｓ６２）。この時の名前解決要求パケットは「Ｇｌｏｂａｌ　Ｅ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」,及び「Ｂ．ｉｎｓｉｄｅ．ｆｕｊｉｔｓｕ．ｃｏｍ」を含む。

【０１８１】

ＤＮＳサーバ１は、ＤＮＳサーバ６から受信した名前解決要求パケットに基づいて通信の可否を判断する。本実施形態では、グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信は禁止しているため、グローバルＩＰアドレス網からの名前解決要求は拒否される。即ち、ＤＮＳサーバ１は、ＤＮＳサーバ６に対して名前解決失敗（ＥＲＲＯＲ）を含む回答パケットを送信する（Ｓ６３）。この場合、送信される回答パケットは「Ｇｌｏｂａｌ　Ｃ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｅ（送信先アドレス）」,及び「ＥＲＲＯＲ（回答）」を含む。

【０１８２】

ＤＮＳサーバ６は、回答パケットを受信すると、サーバ５に対し、名前解決要求パケットに対する回答パケットを送信する（Ｓ６４）。この時、回答パケットは「Ｇｌｏｂａｌ　Ｅ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｄ（送信先アドレス）」,及び「ＥＲＲＯＲ（回答）」を含む。

【０１８３】

サーバ５は、ＤＮＳサーバ６から回答パケットを受信することで、プライベートＩＰアドレス網内に存在する端末２に対する名前解決が出来ないことを知る。

【０１８４】

《Ｉ点におけるＤＮＳサーバ１の動作フロー》

次に、図１４におけるＩ点の処理について、図９を用いて説明する。図９のＳ１００からＳ１０５間は、図３におけるプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信と同じである。従って、図１４に示すグローバルＩＰアドレス網からプライベートＩＰアドレス網への通信については、図９のＳ１０６から説明する。

【０１８５】

Ｓ１０６において、名前解決部１５は、名前解決要求パケットの問合せ元を示すＩＰアドレス（送信元アドレス）がグローバルＩＰアドレス網内のアドレスであり、且つパケットの問合せ先の名前がプライベートＩＰアドレス網内のサーバの名前である場合、即ち、図５の②に該当する場合には、名前解決要求を棄却する（Ｓ１１５）。

【０１８６】

以上は、図１４に示すグローバルＩＰアドレス網からプライベートＩＰアドレス網への通信において、図１４のＩ点におけるＤＮＳサーバ１の動作である。即ち、グローバルＩＰアドレス網からプライベートＩＰアドレス網へ通信において、ＤＮＳサーバ１は、Ｓ１００－Ｓ１０１－Ｓ１０４－Ｓ１０５－Ｓ１０６－Ｓ１１５の順に動作する。

【０１８７】

本発明によれば、ＤＮＳサーバ１は、グローバルＩＰアドレス網からプライベートＩＰアドレス網への通信を禁止（名前解決を拒否）することができ、通常の

ＤＮＳサーバとして機能することができる。

【０１８８】

〔グローバルＩＰアドレス網からグローバルＩＰアドレス網への通信〕

次に、グローバルＩＰアドレス網からグローバルＩＰアドレス網への通信（図５の④に該当）について図１５を用いて説明する。

【０１８９】

図１５は、グローバルＩＰアドレス網からグローバルＩＰアドレス網への通信を示す処理シーケンスである。図１５に示す例では、グローバルＩＰアドレス網において、ＤＮＳサーバ６に“Ｇｌｏａｂａｌ　Ｄ”、サーバ５に“Ｇｌｏｂａｌ　Ｃ（グローバルＩＰアドレス）”と“Ｐｏｒｔ　ＹＹ（ポート番号）”が設定されている。また、プライベートＩＰアドレス網において、端末２に“Ｇｌｏｂａｌ　Ａ（グローバルＩＰアドレス）”と“Ｐｏｒｔ　ＸＸ（ポート番号）”と“名前（Ｂ．ＤＭＺ．ｆｕｊｉｔｓｕ．ｃｏｍ）”が設定されている。また、グレイゾーン上において、ＤＮＳサーバ１に“Ｇｌｏｂａｌ　Ｂ”が設定されている。

【０１９０】

まず、グローバルＩＰアドレス網（The Internet内のネットワーク）に収容されているサーバ５から端末２へパケットを転送する場合には、サーバ５は、端末２のＩＰアドレスを知るために、同一ネットワーク内に存在するＤＮＳサーバ６に名前解決要求パケットを送信する（Ｓ７１）。この場合、送信されるパケットは「Ｇｌｏｂａｌ　Ｃ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｄ（送信先アドレス）」,及び「Ｂ．ＤＭＺ．ｆｕｊｉｔｓｕ．ｃｏｍ（問合せ：名前解決対象の端末２の名前）」を含む。

【０１９１】

次に、ＤＮＳサーバ６は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するＤＮＳサーバ１を送信先アドレスに設定した名前解決要求パケットを送信する（Ｓ７２）。この時の名前解決要求パケットは「Ｇｌｏｂａｌ　Ｄ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｂ（送信先アドレス）」,及び「Ｂ．ＤＭＺ．ｆｕｊｉｔｓｕ．ｃｏｍ」を含む。

【０１９２】

ＤＮＳサーバ１は、ＤＮＳサーバ６から名前解決要求パケットを受信する。すると、名前解決要求パケットに含まれる名前に対応するＩＰアドレスを回答とする回答パケットをＤＮＳサーバ６に返信する（Ｓ７３）。この時、回答パケットは「Ｇｌｏｂａｌ　Ｂ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｄ（送信先アドレス）」,及び「Ｇｌｏｂａｌ　Ａ（回答：名前に対応するグローバルＩＰアドレス）」を含む。

【０１９３】

ＤＮＳサーバ６は、回答パケットを受信すると、サーバ５に対し、名前解決要求に対する回答パケットを送信する（Ｓ７４）。この時、パケットは「Ｇｌｏｂａｌ　Ｄ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」,及び「Ｇｌｏｂａｌ　Ａ」を含む。

【０１９４】

名前解決要求パケットを送信したサーバ５は、ＤＮＳサーバ６から受信した回答パケットの内容から問合せに対する回答が「Ｇｌｏｂａｌ　Ａ」であることを知る。即ち、サーバ５は、問合せた名前（B.DMZ.fujitsu.com）に対応するＩＰアドレスが「Ｇｌｏｂａｌ　Ａ」であることを知る。

【０１９５】

端末２は、「Ｇｌｏｂａｌ　Ａ」を持つサーバ５と通信を開始するために、データパケットを送信する（Ｓ７５）。この場合、データパケットのヘッダには「Ｇｌｏｂａｌ　Ｃ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ａ（送信先アドレス）」,「ＹＹ（送信元ポート番号）」,及び「ＸＸ（送信先ポート番号）」が設定される。

【０１９６】

端末２は、サーバ５からのデータパケットを受信するとサーバ５に対し、データパケットを返信する（Ｓ７６）。この場合、データパケットのヘッダは「Ｇｌｏｂａｌ　Ａ（送信元アドレス）」,「Ｇｌｏｂａｌ　Ｃ（送信先アドレス）」,「ＸＸ（送信元ポート番号）」,及び「ＹＹ（送信先ポート番号）」が設定される。

【０１９７】

《ＤＮＳサーバ１の動作フロー》

次に、図１５のＤＮＳサーバ１の動作について説明する。ＤＮＳサーバ１は、Ｓ１００からＳ１０５間の動作は、図３に示されるプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信と同じであるため説明は省略し、Ｓ１０６から説明する。

【０１９８】

Ｓ１０６において、パケットの問合せ先と問合せ元がいずれもグローバルＩＰアドレス網である場合、即ち、図５の④に該当する場合には、名前解決部１５は、名前・アドレスデータベース（グローバル）１５ｂを検索する（Ｓ１０７）。

【０１９９】

名前解決部１５は、名前・アドレスデータベース（グローバル）１５ｂを検索した結果、該当するＩＰアドレスがヒットした場合には、問合せ元への回答はヒットしたグローバルＩＰアドレスとなり、Ｓ１１２に進む。Ｓ１０７において、名前解決部１５が、名前・アドレスデータベース（グローバル）１５ｂを検索した結果、ミスヒットであった場合には、名前解決失敗としてＳ１１２に進む。

【０２００】

Ｓ１１２では、名前解決回答作成部２０は、ＤＮＳの回答を作成する。作成されたＤＮＳの回答は、送信パケット作成部１２でパケット化され、通信終端部１０経由でネットワーク上に送信される（Ｓ１１１）。

【０２０１】

本発明によれば、ＤＮＳサーバ１は、グローバルＩＰアドレス網からグローバルＩＰアドレス網への通信に対して、グローバルＩＰアドレス網上に存在する通常のＤＮＳサーバとして機能することができる。

【０２０２】

〔プライベートＩＰアドレス網からプライベートＩＰアドレス網への通信〕

次に、プライベートＩＰアドレス網からプライベートＩＰアドレス網への通信（図５の①に該当）について説明する。

【０２０３】

《ＤＮＳサーバ１の動作フロー》

プライベートＩＰアドレス網からプライベートＩＰアドレス網への通信は、図５の①に該当するため、ＤＮＳサーバ１の動作は、図１５のグローバルＩＰアドレス網からグローバルＩＰアドレス網への通信（図５の④に該当）と同様となる。

【０２０４】

本発明によれば、ＤＮＳサーバ１は、プライベートＩＰアドレス網からプライベートＩＰアドレス網への通信に対して、プライベートＩＰアドレス網上に存在する通常のＤＮＳサーバとして機能することができる。

【０２０５】

〈その他〉

本発明は、以下のように特定することができる。

（付記１）　通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、

前記判定手段の判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第２判定手段と、

前記第２判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段と、

を含む名前／アドレス変換装置。（１）

（付記２）　第１ネットワーク及び第２ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別手段と、

前記通信元が前記第１ネットワークに属し且つ前記通信先が前記第２ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索手段と、

前記通信先のアドレスを含む回答を送出する送出手段とを含み、

前記送出手段は、前記通信元が前記第２ネットワークに属し且つ前記通信先が

前記第１ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない

名前／アドレス変換装置。（２）

（付記３）　前記送出手段は、前記第１ネットワークに属する通信元と前記第２ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

付記２記載の名前／アドレス変換装置。（３）

（付記４）　前記第１ネットワークに属する通信元に相当する第１端末に対して前記第２ネットワークに属する通信先に相当する第２端末のアドレスが回答される場合に、前記第１ネットワークと前記第２ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第１ネットワークと前記第２ネットワークとの間のアドレス変換を行う中継装置に対し、前記第１端末と前記第２端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含む

付記２又は３記載の名前／アドレス変換装置。（４）

（付記５）　前記通知手段は、前記中継装置が前記第２端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第２端末の前記第２ネットワークにおけるアドレスを前記第１ネットワークのアドレスに変換するために、前記第２端末に対して仮想的に割り当てられる前記第１ネットワークのアドレスと前記第２端末の前記第２ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記送出手段は、前記第１端末が前記第２端末宛のデータに前記第２端末の前記第１ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第２端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第２端末の前記第２ネットワークにおけるアドレスに変換するために、前記第２端末の前記第１ネットワークにおけるアドレスを含む回答を送出する

付記４記載の名前／アドレス変換装置。（５）

（付記６）　前記通知手段は、前記中継装置が前記第１端末と前記第２端末との

間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、前記第１端末と前記第２端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知する
付記４又は５記載の名前／アドレス変換装置。

（付記７）　前記通知手段は、前記送出手段が前記第２端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知する
付記４～６のいずれかに記載の名前／アドレス変換装置。

（付記８）　名前／アドレス変換装置として機能するコンピュータが、

通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定し、

前記判定ステップの判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定し、

前記第２判定ステップが通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する
ことを含む名前/アドレス変換方法。

（付記９）　名前／アドレス変換装置として機能するコンピュータが、

第１ネットワーク及び第２ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信し、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別し、

前記通信元が前記第１ネットワークに属し且つ前記通信先が前記第２ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索し、

前記通信先のアドレスを含む回答を送出し、

前記通信元が前記第２ネットワークに属し且つ前記通信先が前記第１ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない
ことを含む名前/アドレス変換方法。

（付記１０）　前記コンピュータは、

前記第１ネットワークに属する通信元と前記第２ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

付記９記載の名前/アドレス変換方法。

（付記１１）　前記コンピュータは、

前記第１ネットワークに属する通信元に相当する第１端末に対して前記第２ネットワークに属する通信先に相当する第２端末のアドレスが回答される場合に、前記第１ネットワークと前記第２ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第１ネットワークと前記第２ネットワークとの間のアドレス変換を行う中継装置に対し、前記第１端末と前記第２端末との間を転送されるデータを通過させるための通過情報を通知する

ことをさらに含む付記９又は１０記載の名前/アドレス変換方法。

（付記１２）　前記コンピュータは、

前記中継装置が前記第２端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第２端末の前記第２ネットワークにおけるアドレスを前記第１ネットワークのアドレスに変換するために、前記第２端末に対して仮想的に割り当てられる前記第１ネットワークのアドレスと前記第２端末の前記第２ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記第１端末が前記第２端末宛のデータに前記第２端末の前記第１ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第２端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第２端末の前記第２ネットワークにおけるアドレスに変換するために、前記第２端末の前記第１ネットワークにおけるアドレスを含む回答を送出する

付記１１記載の名前/アドレス変換方法。

（付記１３）　前記コンピュータは、

前記中継装置が前記第１端末と前記第２端末との間での利用が許可されたアプ

リケーションに基づくデータのみを通過させるために、前記第１端末と前記第２端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知する

付記１１又は１２記載の名前/アドレス変換方法。

（付記１４）　前記コンピュータは、

前記第２端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知する

付記１１～１３のいずれかに記載の名前/アドレス変換方法。

（付記１５）　コンピュータを名前／アドレス変換装置として機能させるプログラムまたはこのプログラムを記録した記録媒体であって、

通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定ステップと、

前記判定ステップの判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第２判定ステップと、

前記第２判定ステップが通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答ステップと、

を前記コンピュータに実行させるプログラムまたはこのプログラムを記録した記録媒体。

（付記１６）　コンピュータを名前／アドレス変換装置として機能させるプログラムまたはこのプログラムを記録した記録媒体であって、

第１ネットワーク及び第２ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信ステップと、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別ステップと、

前記通信元が前記第１ネットワークに属し且つ前記通信先が前記第２ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索ステップと、

前記通信先のアドレスを含む回答を送出する送出ステップとを含み、

前記通信元が前記第２ネットワークに属し且つ前記通信先が前記第１ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しないステップと、

を前記コンピュータに実行させるプログラムまたはこのプログラムを記録した記録媒体。

（付記１７）　前記第１ネットワークに属する通信元と前記第２ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しないことを判断するステップを前記コンピュータに実行させる付記１６記載のプログラムまたはこのプログラムを記録した記録媒体。

（付記１８）　前記第１ネットワークに属する通信元に相当する第１端末に対して前記第２ネットワークに属する通信先に相当する第２端末のアドレスが回答される場合に、前記第１ネットワークと前記第２ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第１ネットワークと前記第２ネットワークとの間のアドレス変換を行う中継装置に対し、前記第１端末と前記第２端末との間を転送されるデータを通過させるための通過情報を通知する通知ステップを、

さらに前記コンピュータに実行させる付記１６又は１７記載のプログラムまたはこのプログラムを記録した記録媒体。

（付記１９）　前記中継装置が前記第２端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第２端末の前記第２ネットワークにおけるアドレスを前記第１ネットワークのアドレスに変換するために、前記第２端末に対して仮想的に割り当てられる前記第１ネットワークのアドレスと前記第２端末の前記第２ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知するステップと、

前記第１端末が前記第２端末宛のデータに前記第２端末の前記第１ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第２端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第２端末の前記第２ネットワークにおけるアドレスに変換するため

に、前記第２端末の前記第１ネットワークにおけるアドレスを含む回答を送出するステップとを、
前記コンピュータに実行させる付記１８記載のプログラムまたはこのプログラムを記録した記録媒体。
（付記２０）　前記中継装置が前記第１端末と前記第２端末との間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、前記第１端末と前記第２端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知するステップを、
前記コンピュータに実行させる付記１８又は１９記載のプログラムまたはこのプログラムを記録した記録媒体。
（付記２１）　前記送出ステップが前記第２端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知するステップを、
前記コンピュータに実行させる付記１８～２０のいずれかに記載のプログラムまたはこのプログラムを記録した記録媒体。

【０２０６】

【発明の効果】

本発明によれば、プロキシサーバを用いることなく、ＩＰネットワーク間の境界上にあるＤＮＳサーバとアドレス変換装置を連携させることにより、異なるＩＰネットワーク空間にまたがる通信を実現することが可能となる。

【図面の簡単な説明】

【図１】　従来技術であるＤＮＳの仕組みを示すＤＮＳツリー図である。

【図２】　従来のプライベートＩＰアドレス網からグローバルＩＰアドレス網間通信におけるＤＮＳのフローを示す図である。

【図３】　本発明の実施形態における通信許可時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信を示す図である。

【図４】　プライベートＩＰアドレス網に対するグローバルＩＰアドレス網の見せ方を示す図である。

【図５】　名前解決要求の問合せ元に応じたＤＮＳサーバの回答を示す図である。

【図６】　本発明の実施形態におけるＤＮＳサーバのシステム構成を示す図である。

【図７】　本発明の実施形態におけるアドレス変換・フィルタリング装置のシステム構成を示す図である。

【図８】　本発明の実施形態におけるパケットのデータ構造を示す図である。

【図９】　本発明の実施形態におけるＤＮＳサーバの動作を示すフローチャートである。

【図１０】　本発明の実施形態におけるアドレス変換・フィルタリング装置の動作を示すフローチャートである。

【図１１】　本発明の実施形態におけるプライベートＩＰアドレスの返却処理を示す図である。

【図１２】　本発明の実施形態における名前による通信拒否時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信を示す図である。

【図１３】　本発明の実施形態におけるポートによる通信拒否時のプライベートＩＰアドレス網からグローバルＩＰアドレス網への通信を示す図である。

【図１４】　本発明の実施形態におけるグローバルＩＰアドレス網からプライベートＩＰアドレス網への通信を示す図である。

【図１５】　本発明の実施形態におけるグローバルＩＰアドレス網からグローバルＩＰアドレス網への通信を示す図である。

【符号の説明】

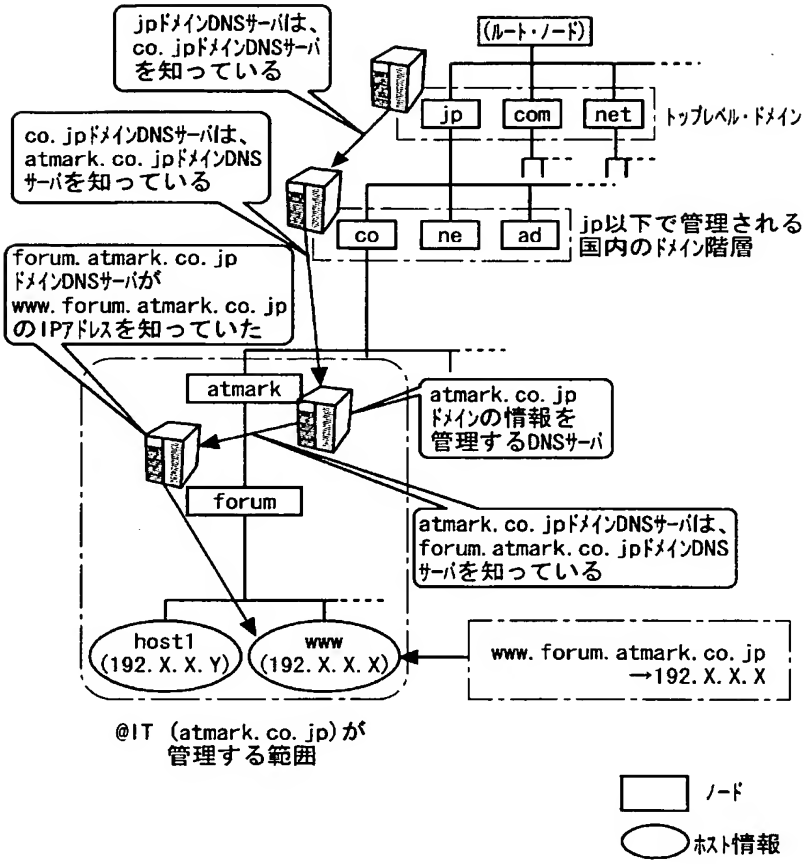
１，４，６	ＤＮＳサーバ
２，５	端末
３	アドレス変換・フィルタリング装置
７	Ｌ２－ＳＷ
８	ルータ
１０	通信終端部
１１	受信識別部
１２	送信パケット作成部

１３	名前解決要求問合せ元識別部
１４	名前解決要求問合せ先識別部
１５	名前解決部
１５ａ，１５ｂ	名前・アドレスデータベース
１６	通信許可ポート検索部
１６ａ	通信許可ポートリスト
１７	アドレス割当部
１８	アドレス返却部
１９	アドレスプール管理部
１９ａ	アドレスプールリスト
２０	名前解決回答作成部
２１	アドレス通知作成部
３１	通信終端部
３２	受信識別部
３３	送信パケット作成部
３４	フィルタ書換え部
３５	アドレス書換え・フィルタデータベース
３６	アドレス書換え・フィルタ部
３７	タイマ部
３８	設定完了通知部
３９	ＮＡＴ部
４０	返却通知作成部
１００	パケット

【書類名】　図面

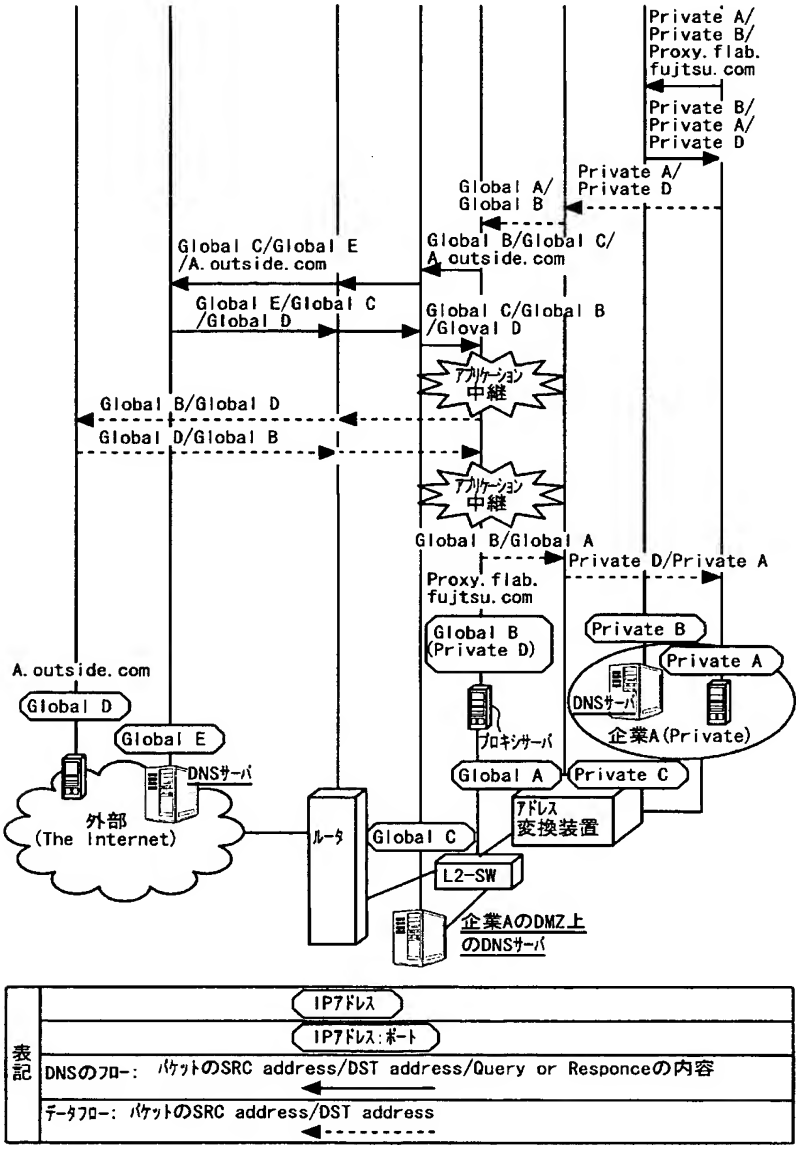
【図１】

ＤＮＳツリー図



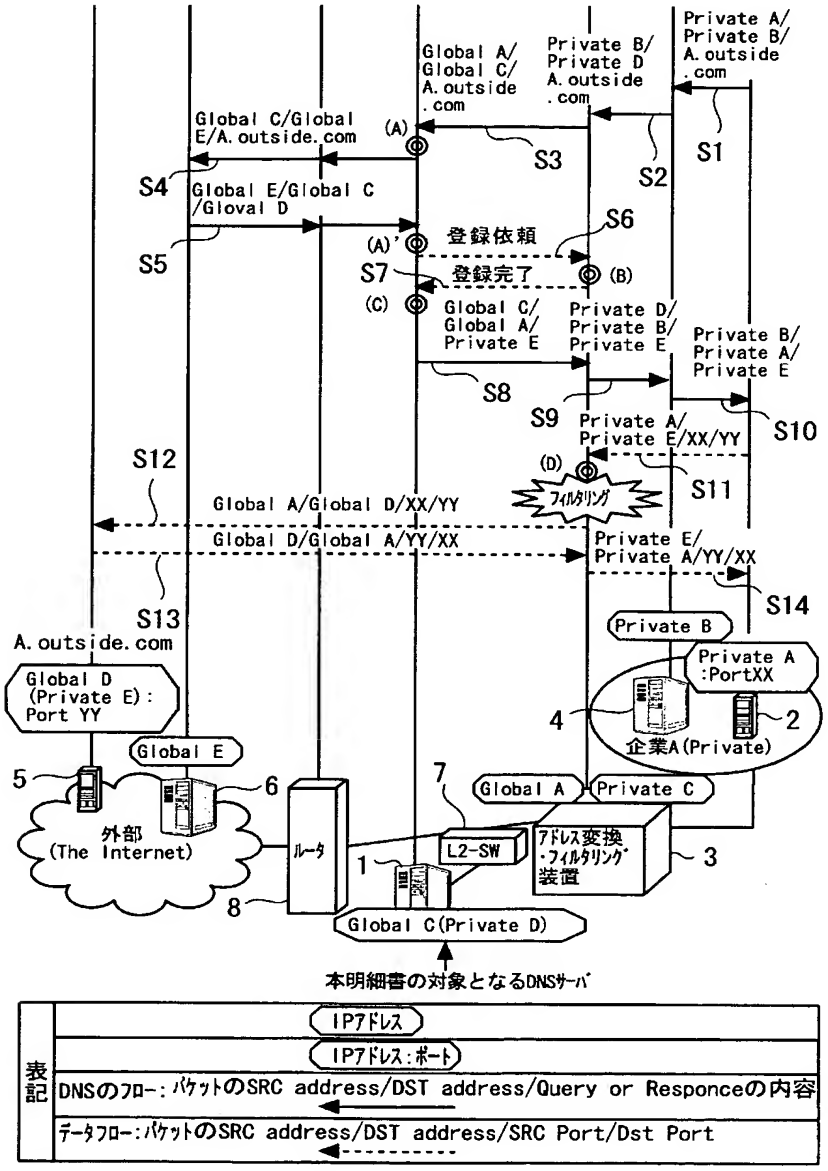
【図２】

プライベートIP網からグローバルIP網間通信におけるDNSのフロー(従来)



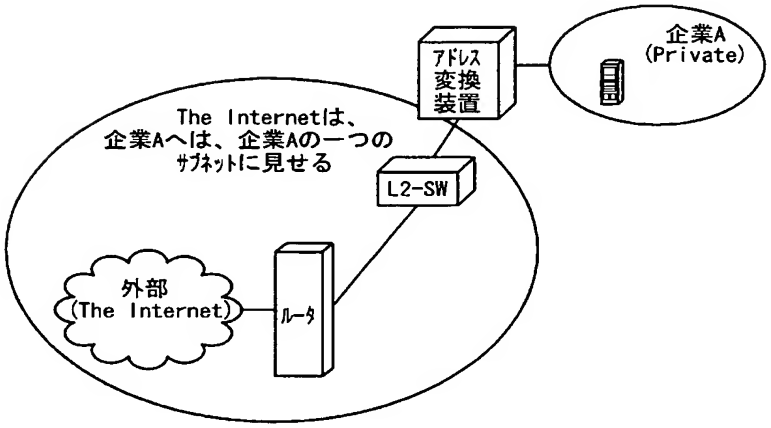
【図３】

プライベートIPアドレス網内からグローバルIPアドレス網への通信フロー図(通信許可時)



【図４】

プライベートIPアドレス網へのグローバルIPアドレス網の見せ方

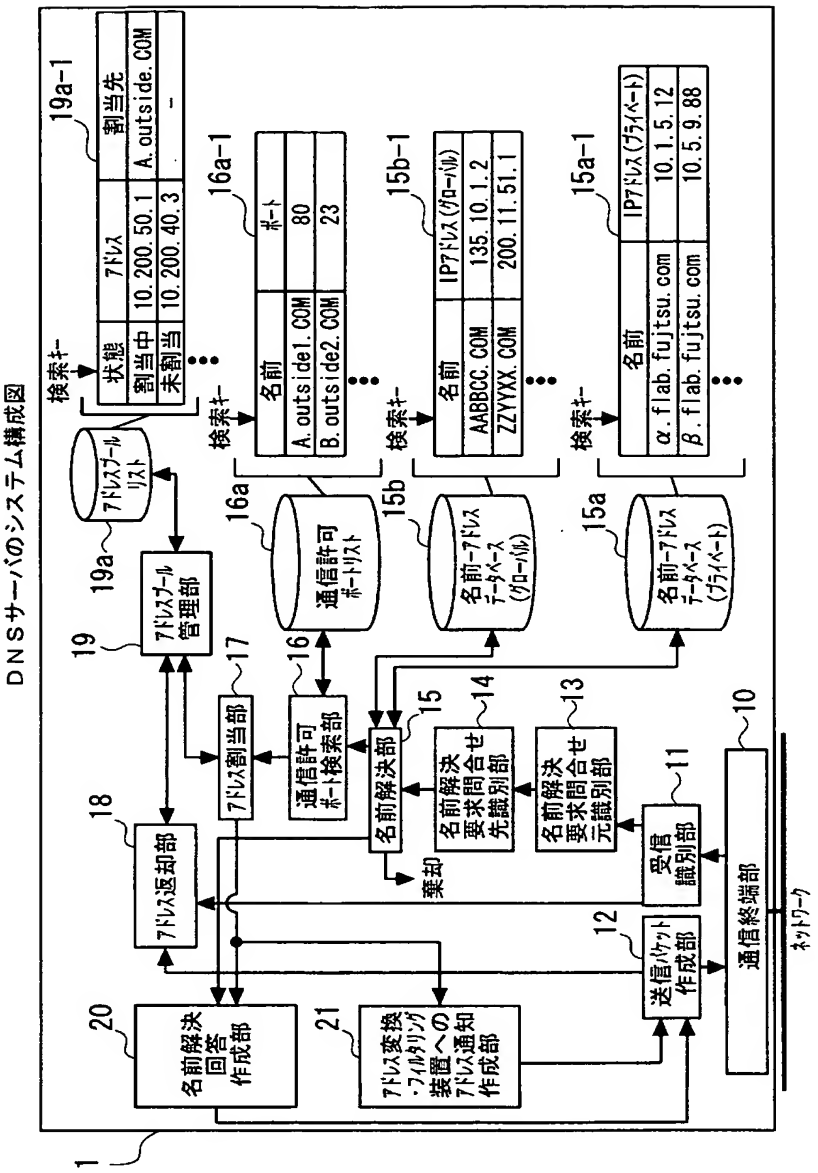


【図５】

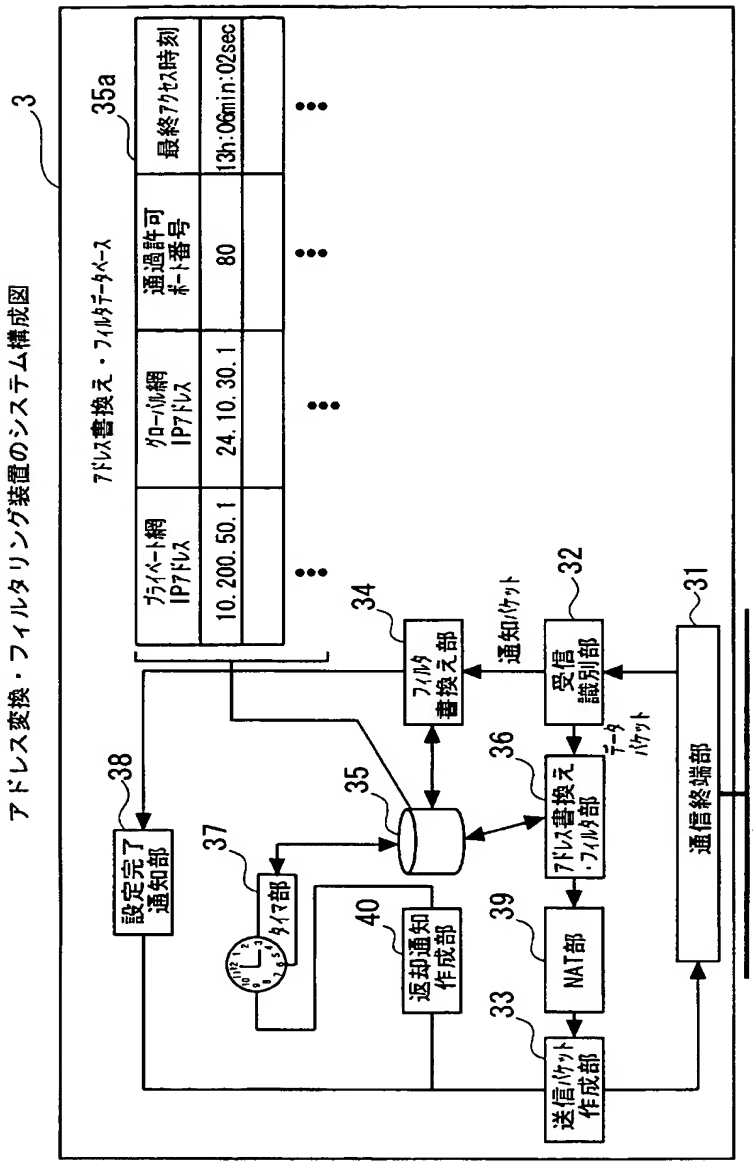
名前解決要求の問合せ元に応じたDNSｻｰﾊﾞの回答

解決する名前の端末位置 ＼ 名前解決要求の問合せ元	ﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽ網	ｸﾞﾛﾊﾞｰﾙIPｱﾄﾞﾚｽ網
ﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽ網	①通常のﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽ網上のDNSｻｰﾊﾞとして動作	②名前解決要求棄却
ｸﾞﾛﾊﾞｰﾙIPｱﾄﾞﾚｽ網	③接続可否を判断の上、回答	④通常のｸﾞﾛﾊﾞｰﾙIPｱﾄﾞﾚｽ網上のDNSｻｰﾊﾞとして動作

【図６】

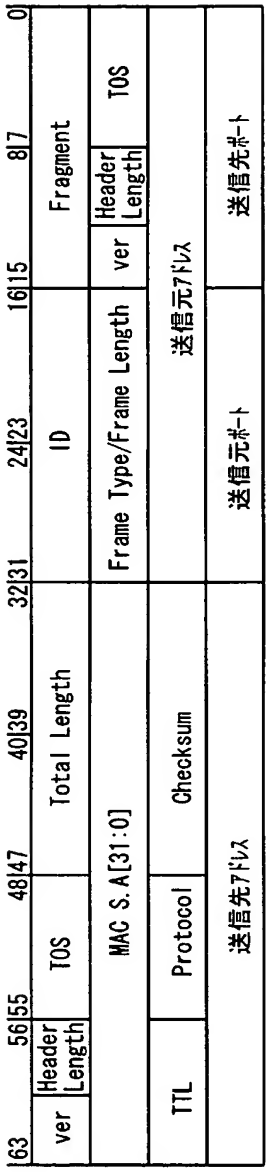

DNSサーバのシステム構成図
1
19a-1
状態
割当中
未割当
アドレス
10.200.50.1
10.200.40.3
割当先
A.outside.COM
-
検索キー
アドレスプール リスト
19a
アドレスプール 管理部
19
16a-1
名前
A.outside1.COM
B.outside2.COM
ポート
80
23
16a
通信許可 ポートリスト
15b-1
名前
AABBCC.COM
ZZYYXX.COM
IPアドレス(グローバル)
135.10.1.2
200.11.51.1
15b
名前-アドレス データベース (グローバル)
15a-1
名前
α.flab.fujitsu.com
β.flab.fujitsu.com
IPアドレス(プライベート)
10.1.5.12
10.5.9.88
15a
名前-アドレス データベース (プライベート)
16
通信許可 ポート検索部
17
アドレス割当部
18
アドレス返却部
15
名前解決部
14
名前解決 要求問合せ 先識別部
13
名前解決 要求問合せ 元識別部
11
受信 識別部
12
送信パケット 作成部
10
通信終端部
ネットワーク
乗却
20
名前解決 回答 作成部
21
アドレス変換 ・フィルタリング 装置への アドレス通知 作成部

【図７】

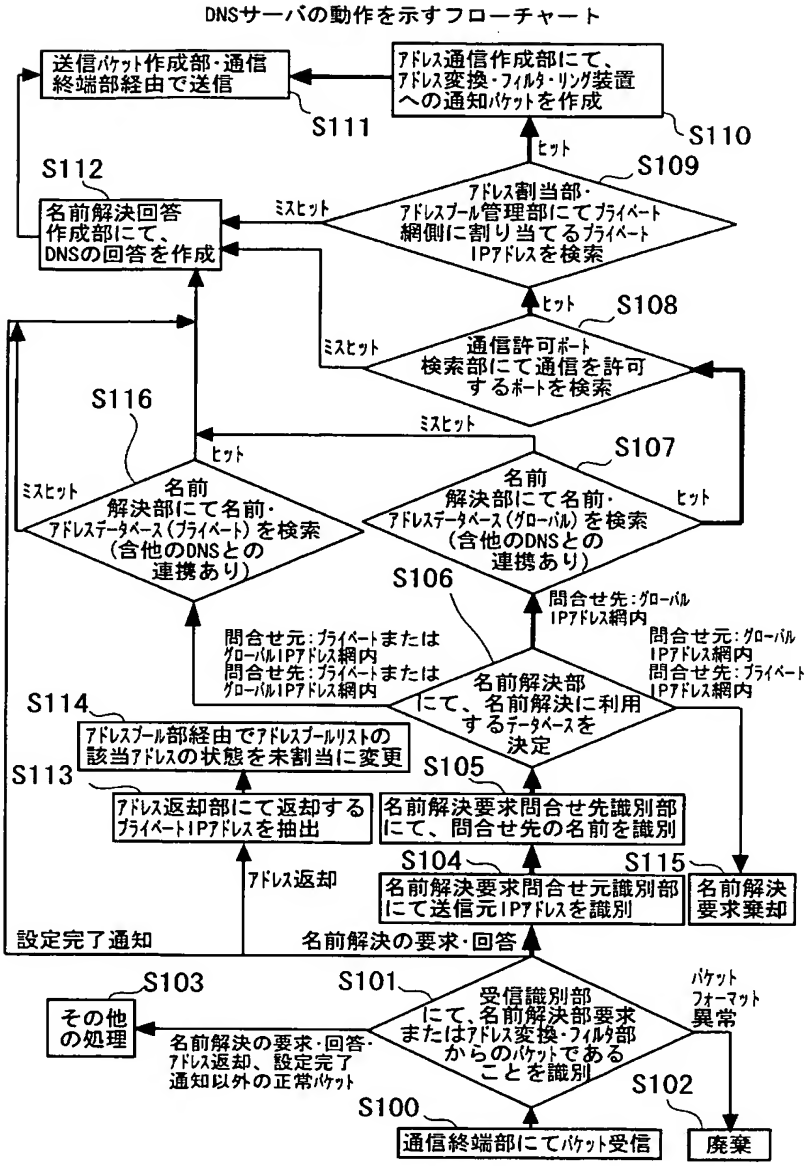

アドレス変換・フィルタリング装置のシステム構成図
3
35a
アドレス書換え・フィルタデータベース
プライベート網IPアドレス
グローバル網IPアドレス
通過許可ポート番号
最終アクセス時刻
10.200.50.1
24.10.30.1
80
13h:06min:02sec
34
フィルタ書換え部
通知パケット
32
受信識別部
31
38
設定完了通知部
37
タイマ部
35
36
アドレス書換え・フィルタ部
データパケット
通信終端部
ネットワーク
40
返却通知作成部
39
NAT部
33
送信パケット作成部

【図８】

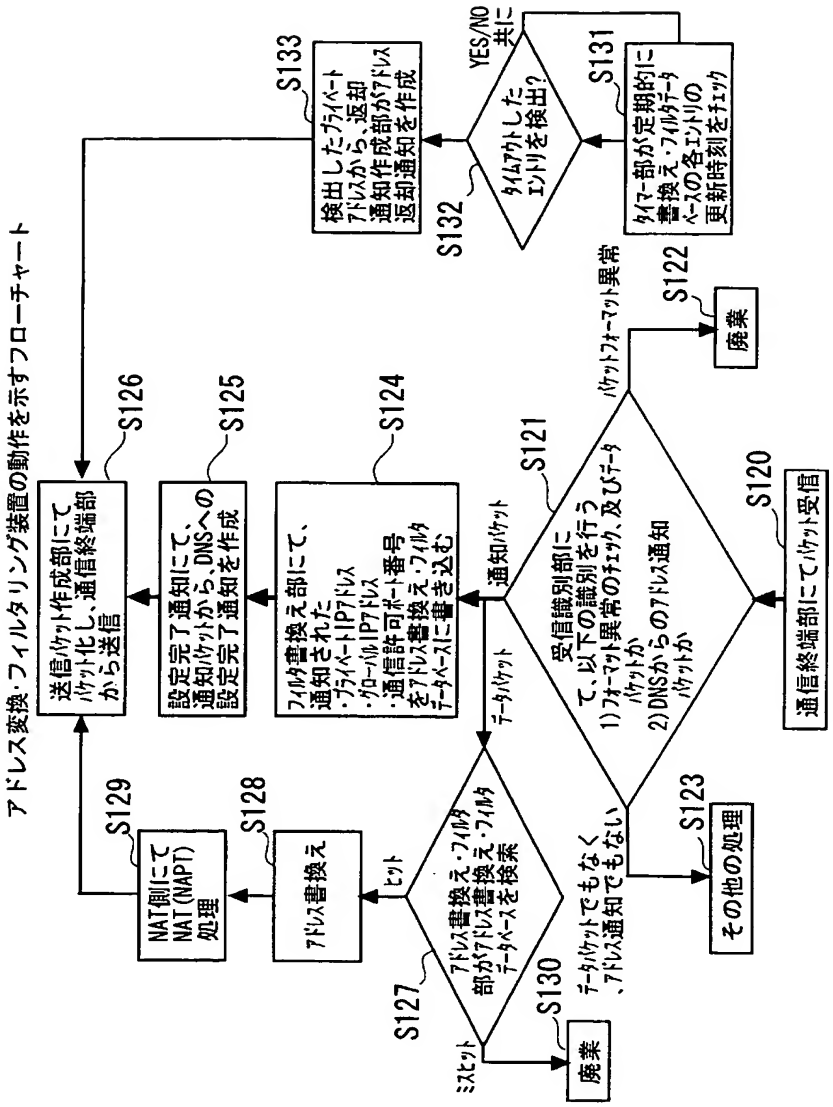
パケットのデータ構造(ヘッダ部)



【図９】

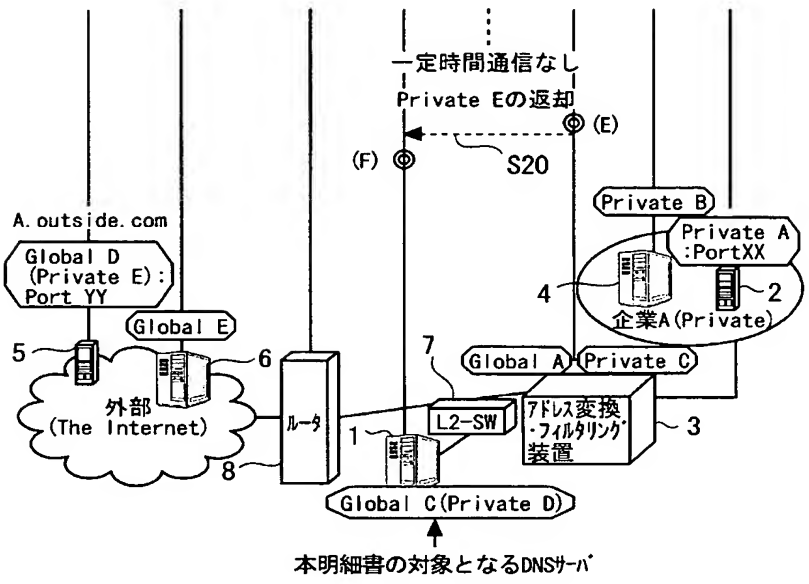

DNSサーバの動作を示すフローチャート
送信パケット作成部・通信終端部経由で送信
S111
アドレス通信作成部にて、アドレス変換・フィルタ・リング装置への通知パケットを作成
S110
ヒット
S109
S112
アドレス割当部・アドレスプール管理部にてプライベート網側に割り当てるプライベートIPアドレスを検索
ミスヒット
名前解決回答作成部にて、DNSの回答を作成
ヒット
S108
ミスヒット
通信許可ポート検索部にて通信を許可するポートを検索
S116
ミスヒット
S107
ヒット
ミスヒット
名前解決部にて名前・アドレスデータベース（プライベート）を検索（含他のDNSとの連携あり）
名前解決部にて名前・アドレスデータベース（グローバル）を検索（含他のDNSとの連携あり）
ヒット
S106
問合せ先：グローバルIPアドレス網内
問合せ元：プライベートまたはグローバルIPアドレス網内
問合せ先：プライベートまたはグローバルIPアドレス網内
問合せ元：グローバルIPアドレス網内
問合せ先：プライベートIPアドレス網内
名前解決部にて、名前解決に利用するデータベースを決定
S114
アドレスプール部経由でアドレスプールリストの該当アドレスの状態を未割当に変更
S113
S105
アドレス返却部にて返却するプライベートIPアドレスを抽出
名前解決要求問合せ先識別部にて、問合せ先の名前を識別
S104
S115
アドレス返却
名前解決要求問合せ元識別部にて送信元IPアドレスを識別
名前解決要求棄却
設定完了通知
名前解決の要求・回答
S103
S101
パケットフォーマット異常
その他の処理
受信識別部にて、名前解決部要求またはアドレス変換・フィルタ部からのパケットであることを識別
名前解決の要求・回答・アドレス返却、設定完了通知以外の正常パケット
S102
S100
通信終端部にてパケット受信
廃棄

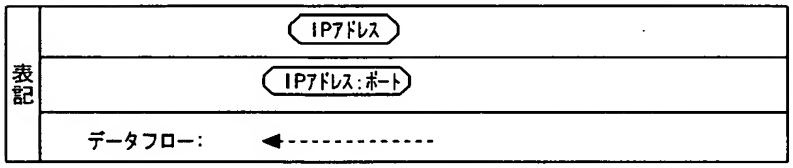
【図１０】


アドレス変換・フィルタリング装置の動作を示すフローチャート
S133
検出したプライベート
アドレスから、返却
通知作成部がアドレス
返却通知を作成
YES/NO
共に
S132
タイムアウトした
エントリを検出?
S131
タイマー部が定期的に
書換え・フィルタデータ
ベースの各エントリの
更新時刻をチェック
S126
送信パケット作成部にて
パケット化し、通信終端部
から送信
S125
設定完了通知にて、
通知パケットから、DNSへの
設定完了通知を作成
S124
フィルタ書換え部にて、
通知されたプライベートIPアドレス
・グローバルIPアドレス
・通信許可ポート番号
をアドレス書換え・フィルタ
データベースに書き込む
通知パケット
S121
受信識別部にて、以下の識別を行う
1) フォーマット異常のチェック、及びデータパケットか
2) DNSからのアドレス通知パケットか
パケットフォーマット異常
S122
廃棄
S120
通信終端部にてパケット受信
S129
NAT側にて
NAT(NAPT)
処理
S128
アドレス書換え
ヒット
S127
アドレス書換え・フィルタ
部がアドレス書換え・フィルタ
データベースを検索
データパケット
S123
データパケットでもなく、
アドレス通知でもない
その他の処理
ミスヒット
S130
廃棄

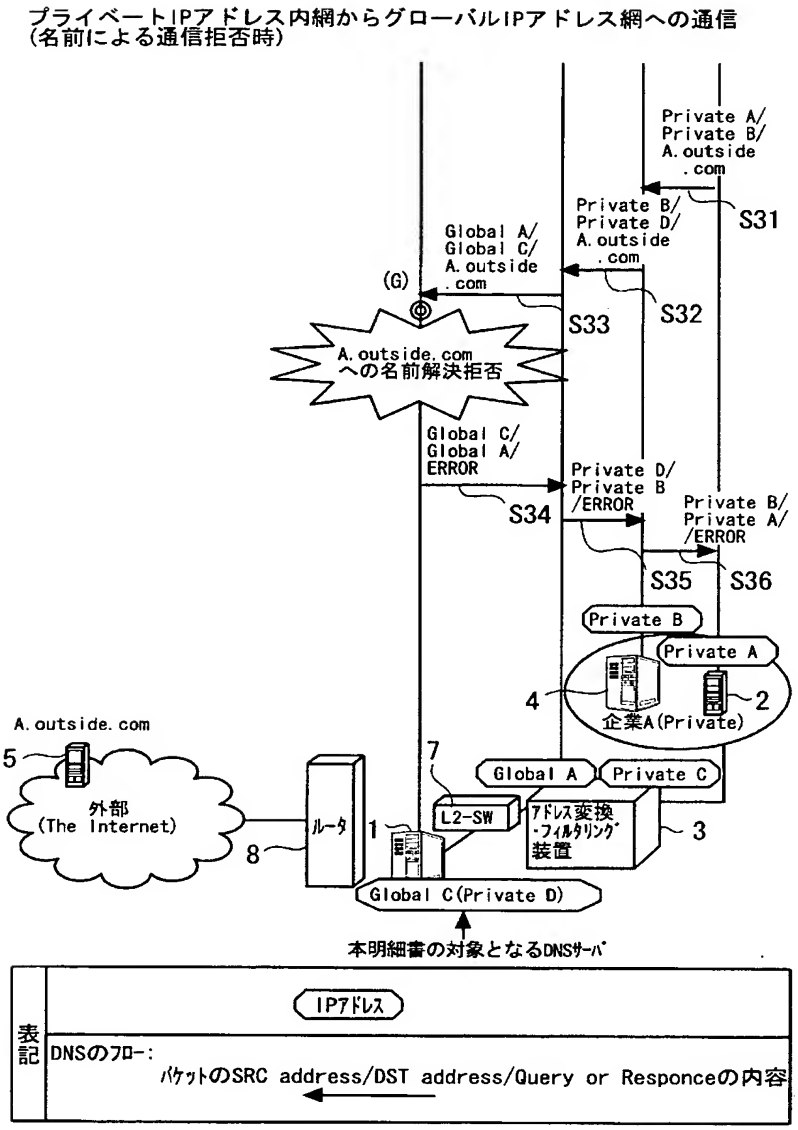
【図１１】

プライベートIPアドレスの返却時のフロー

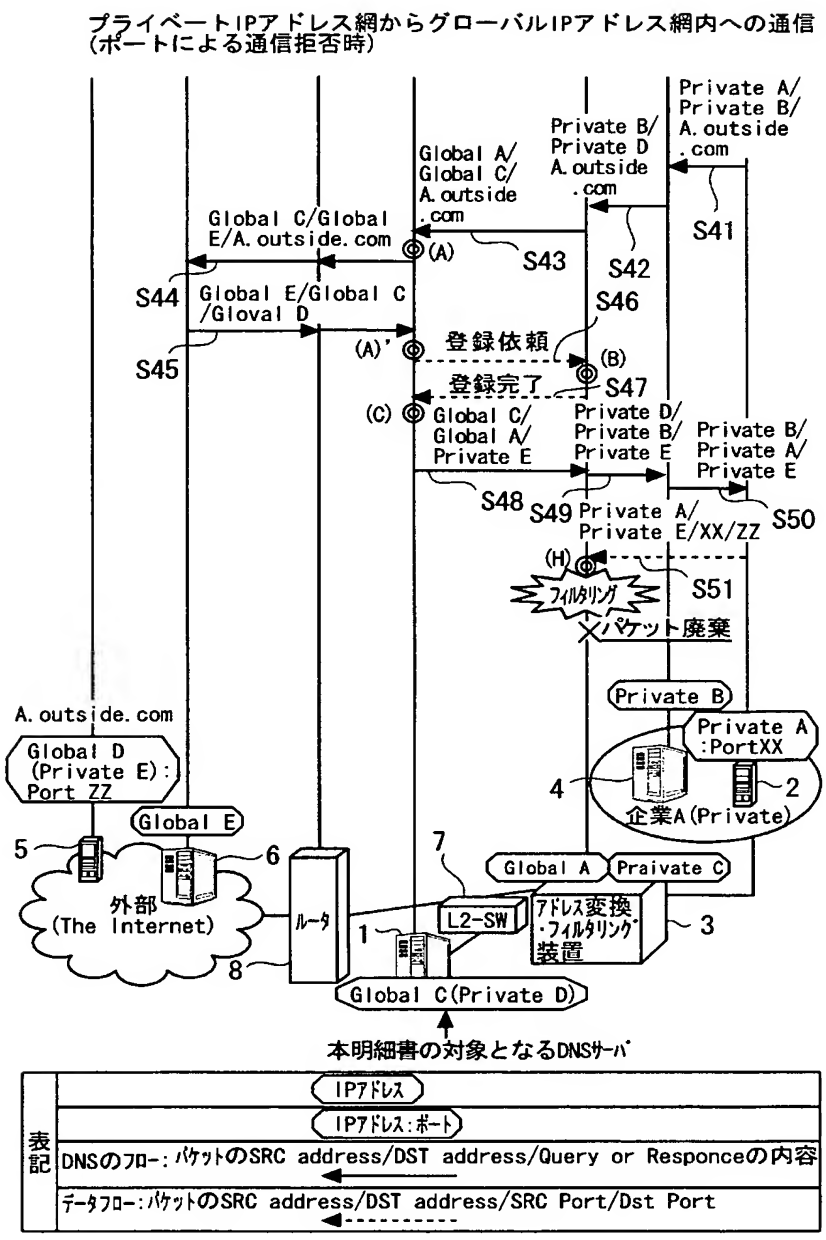




【図１２】

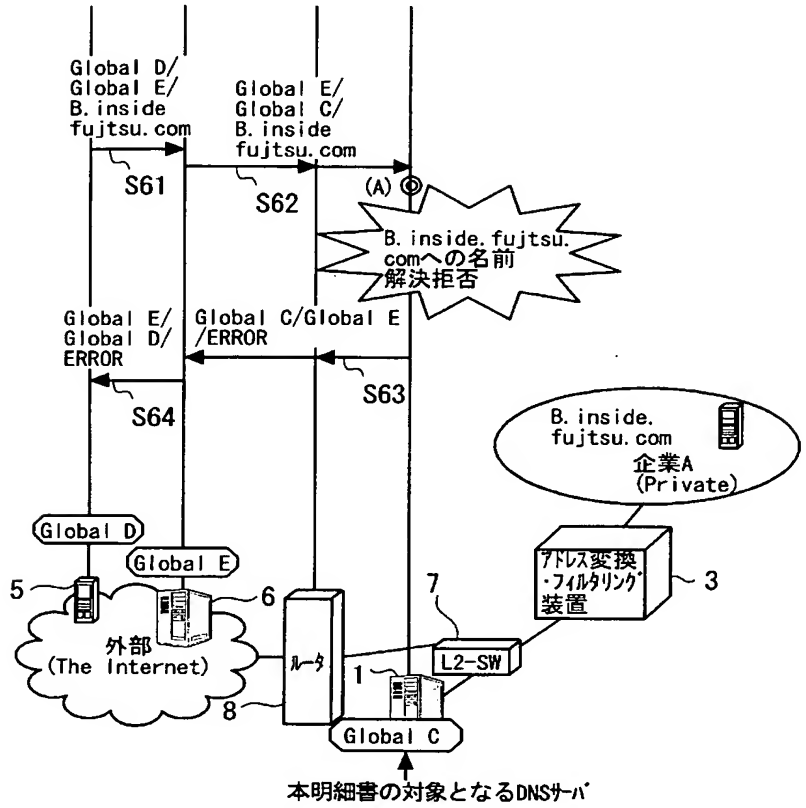

プライベートIPアドレス内網からグローバルIPアドレス網への通信
(名前による通信拒否時)
Private A/
Private B/
A.outside
.com
S31
Private B/
Private D/
A.outside
.com
S32
Global A/
Global C/
A.outside
.com
(G)
S33
A.outside.com
への名前解決拒否
Global C/
Global A/
ERROR
S34
Private D/
Private B
/ERROR
S35
Private B/
Private A/
/ERROR
S36
Private B
Private A
4
2
企業A(Private)
A.outside.com
5
外部
(The Internet)
8
ルータ
1
7
Global A
Private C
L2-SW
アドレス変換
・フィルタリング
装置
3
Global C(Private D)
本明細書の対象となるDNSサーバ
表記
IPアドレス
DNSのフロー:
パケットのSRC address/DST address/Query or Responceの内容

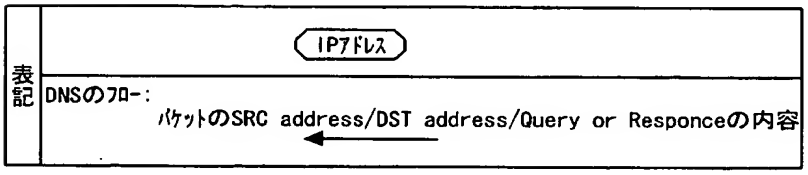
【図１３】


プライベートIPアドレス網からグローバルIPアドレス網内への通信
(ポートによる通信拒否時)
Private A/
Private B/
A.outside
.com
Private B/
Private D
A.outside
.com
Global A/
Global C/
A.outside
.com
Global C/Global
E/A.outside.com
(A)
S41
S42
S43
S44
Global E/Global C
/Gloval D
S45
S46
(A)'
登録依頼
(B)
登録完了
S47
(C)
Global C/
Global A/
Private E
Private D/
Private B/
Private E
Private B/
Private A/
Private E
S48
S49
Private A/
Private E/XX/ZZ
S50
(H)
S51
フィルタリング
パケット廃棄
Private B
Private A
:PortXX
4
2
企業A(Private)
A.outside.com
Global D
(Private E):
Port ZZ
Global E
5
6
7
Global A
Praivate C
外部
(The Internet)
ルータ
L2-SW
アドレス変換
・フィルタリング
装置
3
1
8
Global C(Private D)
本明細書の対象となるDNSサーバ
表記
IPアドレス
IPアドレス:ポート
DNSのフロー:パケットのSRC address/DST address/Query or Responceの内容
データフロー:パケットのSRC address/DST address/SRC Port/Dst Port

【図１４】

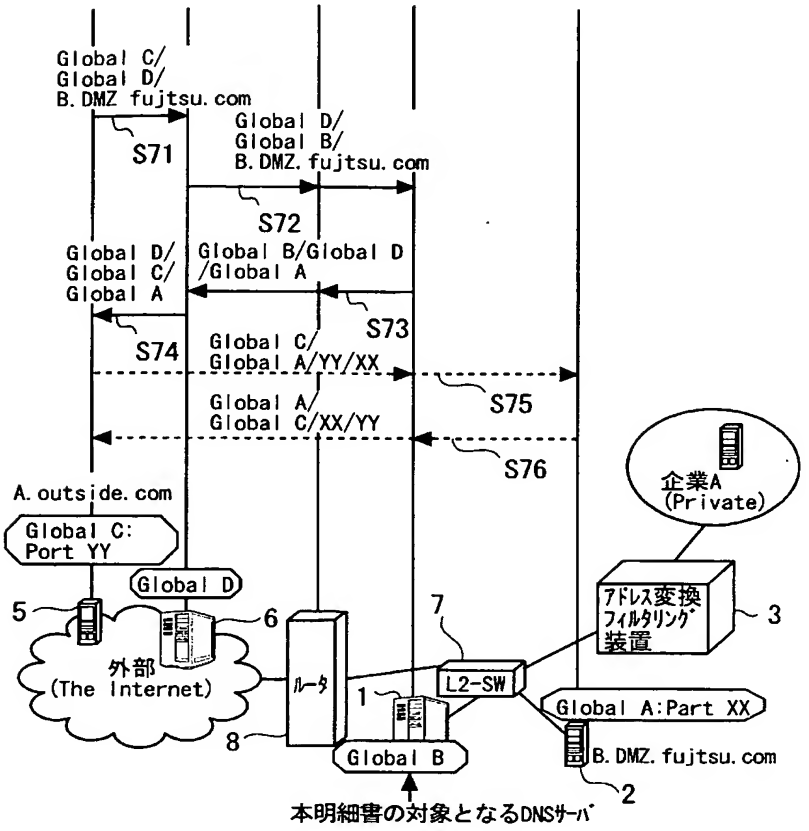
グローバルIPアドレス網からプライベートIPアドレス網への通信

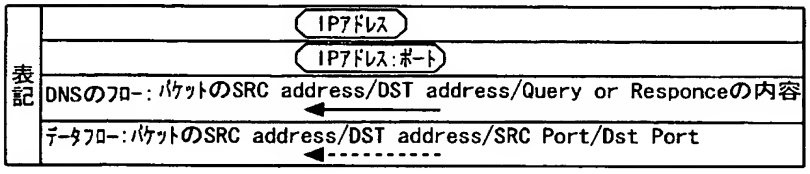




【図１５】

グローバルIPアドレス網からグローバルIPアドレス網への通信





【書類名】　要約書

【要約】

【課題】　異なるＩＰネットワーク間にまたがる通信をプロキシサーバを用いることなく実現することができる装置や方法を提供する。

【解決手段】　名前／アドレス変換装置は、通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、上記判定手段の判定結果に基づいて、上記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第２判定手段と、上記第２判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段とを含む。

【選択図】　図６

特願２００３－０９１２９３

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社